fridolin

der bitverwurstler

nummer 35 die zeitschrift für verwirrte informatikerInnen Mai/Juni 88

hacken

Wettbewerb

Künstliche Kunst

Prämiert werden die besten Programme, die selbständig "Kunstwerke" (etwa Bilder, Dichtung, Musik, Animation,...) genererieren.
Dabei wird der künsterlische Anspruch bewertet werden und nicht etwa die Komplexität des Algorithmus oder dessen Eleganz. Entscheidend ist alleine der "Output".
Die besten Werke werden dann in einer Ausstellung zum Thema "künstliche Kunst" anläßlich der 16.5ten KiF in Wien gezeigt. Weitere Ausstellungsobjekte werden sein: computergesteuerte Maschinen, Animationsvideos, Dokumentationen von Netzwerkprojekten, Texte über die Ästhetik der Maschine,...
Veranstalter dieses Wettbewebs und auch der Ausstellung ist der Verein der InformatikstudentInnen (Fachschaft Informatik) mit Unterstützung der Österreichischen Computergrafik—Gesellschaft (ACGA).
Wir suchen zur Bewältigung des administrativen Chaos auch noch einige Mitarbeiter.

Inhalt dieses extradicken fridolin ist zB:

IMPRESSUM

Medieninhaber, Herausgeber und Verleger: FACHSCHAFT INFORMATIK 1040 Wien, Karlsplatz 13 Druck: Eigenverfielfältigung

Die Chipkarte

Der direkte Weg zur gläsernen Gesellschaft

In den nächsten Jahren wird eine kleine Karte, so groß wie die Scheckkarte, unseren Alltag prägen.

Durch einen eingebauten Mikroprozessor erfüllt sie zahlreiche Funktionen und ist universell einsetzbar. Die Chipkarte wird als Ausweis dienen, sozusagen als "elektronischer Schlüssel" den Bankomat-tresor öffnen und ihm die Auszahlung einer bestimmten Summe befehlen, die Zapfsäule an der Selbstbedienungstankstelle zur Funktion bringen und auch die Kinokarte bezahlen. Es wird möglich sein, eine vollständige Krankengeschichte in einen durch Code gesicherten Geheimbereich zu speichern, und der Medikamentenbedarf wird vom Apotheker abgelesen. Das "Kärtchen" ist auch imstande, das Studienbuch eines Studenten zu speichern, und aufgrund des Datenschutzes hat jeder Professor nun Zugriff auf "seinen" Speicher. Natürlich wird man auch mit dieser Karte telefonieren und vom Automaten Flugtickets kaufen können. Der Automat informiert, bucht und verkauft.

Dieser Exkurs in die Zukunft ist keine Utopie, denn der Weg zur einheitlichen Chipkarte ist bereits von Wissenschaft und Technik mit zahlreichen Versuchen abgesteckt.

Seit zwei Jahren werden Chipkarten mit den o.g. Einsatzmöglichkeiten in Frankreich an jeden Haushalt ausgegeben. Von den Pariser Bürgersteigen sind bereits die letzten Parkuhren verschwunden. In Zukunft werden die Autofahrer die Parkgebühren mit Hilfe ihrer Chipkarte bezahlen können.

In wenigen Jahren, so meinen Fachleute, wird die Chipkarte sich in den Industrieländern durchgesetzt haben. Die Entwicklungszeiten der neuen Technologien werden immer kleiner. Die Vorläufer sind bereits historisch: Fahrkartenautomaten für Massenverkehrsmittel, die allerdings noch mit Münzen gespeist werden und hauptsächlich auf elektromechanischer Basis arbeiten, sind heute bereits selbstverständlich geworden. Ein Schritt in Siebenmeilenstiefeln ist die Telefonwertkarte. Nach jedem Gespräch wird die Gebühr in Zeit und Entfernungseinheiten abgebucht.

Das angepeilte Ziel bei Flug- oder Hotelbuchungen ist die Do-it-yourself-Bedienung. Der Kunde informiert sich, bucht, kauft und fertigt sich selbst ab.

Erste Schritte in Österreich sind bereits getätigt worden. Neben der Telefonwertkarte kann man bereits mit der Bankomatkarte bei einigen Tankstellen den zu zahlenden Betrag abbuchen lassen Weiters ist ein europaweites einheitliches Bankomatnetz im Aufbau, in dem bis 1991 bei jedem Geldausgabeautomat in Europa Bares an jeden beliebigen Kartenbesitzer ausgespuckt wird. Und bis 1993 sollte nach dem "european accord" (so die offizielle Bezeichung dieses Plans) auch Wirklichkeit werden, was für heimische Bankomatkarteneigner bisher nur im Inland und nur an wenigen Tankstellen oder Fotofilialen möglich ist: der bargeldlose Einkauf mittels Chipkarte an allen elektronischen Kassen Europas.

Welche sozialen Konsequenzen ergeben sich nun aus dieser Entwicklung? Ansatzweise skizziere ich hier zwei Schwerpunkte.

- Was den Dienstleistungssektor betrifft, also die Bereiche Bankgeschäfte, Hotel-, Flugbuchungen u.ä., wird es zu einer massiven Reduzierung des Dienstleistungspersonals kommen, wobei Frauen in diesen Bereichen besonders stark betroffen sein werden. Darüberhinaus verursacht die Verlagerung dieser Tätigkeiten in den privaten Bereich zusätzliche Belastungen und Zeitaufwendungen für den "Kunden".
- Die zweite soziale Konsequenz ist die totale Überwachungs- und Kontrollmöglichkeit über jeden Einzelnen. Auf die Minute genau, wie schon auf Restaurantabrechnungen (s. Faksimile), können Tagesabläufe, ja ganze Lebensläufe einzelner Personen nachvollzogen und durchleuchtet werden. Was jetzt auf einem Stück Papier (z.B. der Restaurantrechnung) steht und nicht so leicht auswertbar erscheint, wird mittels einer mikroprozessorgesteuerten Chipkarte zu sensiblen, verknüpfbaren, personenbezogenen Daten. Und da kann es durchaus vorkommen, daß aufgrund der gespeicherten Gesundheitsdaten und der leicht erkennbaren Lebensgewohnheiten der Antrag auf eine Lebensversicherung abgelehnt wird, ohne daß der Antragsteller eigentlich genau weiß, warum. Die Kontrolle über die Chipkarte geht für den Betroffenen unweigerlich verloren.

Der gläserne Bürger, die gläserne Gesellschaft ist bereits in Ansätzen Realität und wird mit einer solchen Chipkarte nur weiter ausgebaut.

Othmar Brigar

```
ROSENBERGER BETR GMBH & COKG
  7411 LOIPERSDORF/PINKAFELD
 49000     2      12.05.1988

     16# KELLNER 16
RADLER 0.5 L     2        29.00
 SCHW-SCHN.GE    1        89.00
ERDBEERTORTE     1        30.00
 ZW-SUMME                148.00

 MWST-BRUTTOUMSATZ       148.00
10.00% MWST  1    10.82
    NETTOUMSATZ  108.18
20.00% MWST  2     4.83
    NETTOUMSATZ   24.17

 BAR                     200.00
RUECKGELD                52.00

!! VIELEN DANK  GUTE FAHRT !!
 BON-NR./    UHRZEIT/KASSIERER
2733          13:05        2
```

Quo vadis, Grünbacher?

Am 4.Mai kam Prof. Grünbacher zu uns in die Fachschaftssitzung, um uns sein Konzept zur Umgestaltung seiner Massenlehrveranstaltungen zu präsentieren.

Er ist nämlich von dieser Unterrichtsform gar nicht begeistert und hat sich einen Ausweg einfallen lassen. Der heißt CAI – Computer Aided Instructing.

Vor seinem geistigen Auge schwebt ein Szenario, in dem StudentInnen vor Workstations oder Terminals in den eigenen vier Wänden Lernrationen über ISDN abrufen (oder, für die Altmodischen unter uns, mittels Diskette nach Hause tragen) und studieren. So hofft er,wird etwa ein Drittel bis die Hälfte einer Lehrveranstaltung durch Courseware ersetzt.

Die erste Stufe, so Grünbacher, stellt ein Labor dar, in dem für eine Lehrveranstaltung pro 20 Studenten ein Rechner steht. Diese Rechner sind klarerweise vernetzt. Dort können sich dann die StudentInnen ihre computergestützten Lehreinheiten geben. Die Lehr-Software kann außerdem von jedem mitgenommen (Freeware) und daheim am eigenen Rechner (einen AT mit EGA-Karte und Luxusbildschirm hat ja eh schon fast jeder Informatikstudent, sagt er) verwendet werden. Durch die Vernetzung ist es außerdem möglich, aktuelle Daten wie Prüfungsergebnisse, Termine oder Korrekturen zum Skriptum abzurufen (klarerweise kann man das in fernerer Zukunft auch vom Computer zu Hause aus tun). Verlockend, oder nicht?

Er sieht dadurch auch eine erweiterte Kontrollmöglichkeit für StudentInnen. Er/Sie bekommt einen besseren Überblick darüber, wohin seine Zeit geht und wozu mensch arbeitet.

Probleme sieht Prof. Grünbacher keine, auch wenn er meint, daß, falls sich die ganze Sache als Flop erweist, er sie wieder versterben lassen wird.
Das System, das er einsetzen möchte heißt übrigens COSTOC (Computer Supported Teaching Of Computer Science). Systeme dieser Art sind bisher in den USA, der BRD, Kanada, Graz, Linz und an der UNI Wien installiert. Wie der Name bereits vermuten läßt, sidn die meisten verfügbaren Lektionen englisch. Trotzdem hat dieses System einen österreichischen Autor, Prof. Gruber aus Graz, dem wir schon die segensreiche Entwicklung des MUPID verdanken.

Ich sehe in diesen Systemen eine höchst bedenkliche Entwicklung der Lehre an der Universität. Massenuni hin, Massenuni her, dieser Weg führt nicht hinaus. Konkrete Alternativen wie zB. das Projektstudium bieten hier einen weitaus attraktiveren Ausweg. Studien aus der BRD zeigen, daß Projektstudien meist nicht teurer sind als eine vergleichbare Ausbildung im herkömmlichen Sinne.

Bisher installierte Beispiele von CAI-Systeme zeigen auch deutlich deren Schwächen. Das an der TU angebotene PLATO (Computergestützter Unterricht in FORTRAN) ist in dieser Beziehung wohl ein repräsentativer Kandidat. Solch ein System kann von jemand, der es kennt, nur als "lästig" bezeichnet werden (PLATO kann in Form einer Lehrveranstaltung genossen werden).

Auch an der WU ist seit einiger Zeit ein über BTX laufendes System installiert. Der absolute Mißerfolg dieses Systems gibt uns zu denken. Dazu Prof. Grünbacher sinngemäß: Das funktioniert nicht, weil als Zentralrechner eine SIEMENS-Anlage verwendet wird, deren Betriebssystem für diese Aufgabe nicht geeignet ist. Außerdem sei es modisch, gegen jede Neuerung in diesem Bereich zu schimpfen.

Eine Einsatzmöglichkeit als zusätzlich zur LV angebotene Nachschlagemöglichkeit ist ebenfalls relativ absurd: Untersuchungen zeigen, daß bei dem (etwa equivalenten) Problem der Onlinemanuals etwa die doppelte (!) Suchzeit (verglichen mit "herkömmlichen" Handbüchern) notwendig ist, um eine gesuchte Information zu finden. Oder um es klarer zu formulieren: Ich lese unendlich viel lieber in einem guten Buch, in dem ich nach belieben vor- und zurückblättern kann und Teile doppelt lesen und und ... als vom Bildschirm, vor dem ich zusätzlich durch mangelhafte Bildqualität, Strahlung u.ä. belastet werde. Ich lausche noch viel lieber einem guten Vortragenden, als Lehrsoftware abzurufen. Prof. Grünbacher meint, daß sich bestimmte Bereiche zum Vortrag nicht eignen oder für den Computergestützten Unterricht geradezu prädestiniert sind. Als Beispiele führt er

Algorithmen (zB. Sortieralgorithmen) oder die Funktion einer CPU an (dazu zeigte er uns auch ein hochpeinliches Beispiel für dieses COSTOC-System). Interessanterweise ist aber die Vorlesung von Prof. Barth (Algorithmen und Datenstrukturen) eine wirklich gut besuchte, weil qualitativ Hochwertige Vorlesung (eine der wenigen, in die ich vom Anfang bis zum Schluß besucht habe), und Prof. Pangratz zeigt alljährlich in "Logische Schaltkreise", daß auch Gatter mit interessanten Hilfsmitteln aufbereitbar sind und übertrifft damit jede Lehrsoftware um Zehnerpotenzen.

Es treten meiner Meinung nach bei dieser Unterrichtsform auch Probleme sozialer Natur auf. Wenn alle Studenten über kurz oder lang ihre Unterrichtseinheiten zuhause abrufen, verschwinden soziale Strukturen wie spontan gebildete Gruppen oder Lerngemeinschaften völlig von der Bildfläche. Obwohl Prof. Grünbacher die Gruppenarbeit sehr am Herzen liegt, würde er sie dadurch völlig ausrotten. Es gäbe dann nur noch syntetische Gruppen, die bei Übungen zwangsweise zusammengeschweißt werden. Längst wissen wir, daß der Computer ein relativ "egoistisches" Medium ist. Ein Rechner kann nur von einer Person bedient werden, nur eine/r tippt und bestimmt damit den Ablauf der Sache.

Weiters sehe in der Vernetzung aller Rechner eine erweiterte Kontrollmöglichkeit für Professoren. Und wenn auch niemand diese Möglichkeit wahrnimmt, um sich nicht die Finger zu verbrennen, so entsteht doch eine Aura der Überwachung, die in weiterer Folge Unsicherheit und Mißtrauen wachsen läßt.

Fachschaftsseminar 1988

Unser diesjähriges Fachschaftsseminar fand im April in Drosendorf statt.Bei schönem Wetter in angenehmer landschaftlicher Umgebung (beides konnten wir nur wenig ausnützen) verbrachten wir zwei Tage mit Arbeit und Diskussionen über die zukünftige Fachschaftsarbeit.
Bevor ich einige Ergebnisse präsentieren werde, möchte ich zunächst die Teilnehmer kurz aufzählen: Klaus R., Klaus K., Peter, Lukas, Evi, Hannes, Stephan, (studieren Informatik), Astrid (Wirtschaftsinformatik), Anita, Armin, Walter, Bernie, Adina, Johi (Informatik), Martin, Edith (Datentechnik).
Da die Erwartungen an das Seminar sehr verschieden und vielfältig waren, kamen wir bald vom eigentlichen Diskussionsstil ab, um mittels Brainstorming die verschiedenen Fragen, Problemkreise über die Fachschaft und neue Ideen von allen Teilnehmern zu erhalten. Das daraus resultierende Ergebnis war eine lange (im weiteren Verlauf lang zu behandelnde) Liste von Fragen, Anregungen, Vorstellungen über Fachschaftsarbeit und die Organisation in der Fachschaft (Wer tut was? Was soll alles getan werden?...). Wir mußten leider feststellen, daß viele Teilnehmer nichts über die Fachschaft wußten, und somit war eines der herausragenden Themen die Verbesserung des Informationsflusses innerhalb der Fachschaft (Berichte über diverse Kommissionen, Aktivitäten, Kontakte zu anderen Fachschaften, ...) und damit verbunden eine Reorganisation der Fachschaftssitzung, die ja eigentlich u.a. dem Informationsaustausch dienen sollte. Die Einrichtung und Erhaltung eines Archives mit allen Protokollen diverser Kommissionen (Stuko´s, ...), Gedächtnisprotokolle (über Gespräche mit Professoren,...) und Material über alle Aktivitäten soll der Kontinuität in der Fachschaft dienen.
Damit ist es natürlich noch nicht getan, auch andere Themen (vor allem politische Aktivitäten in der Fachschaft) wurden zwar angesprochen, konnten aber aufgrund mangelden Wissens -"Was ist Fachschaftsarbeit eigentlich? "- und größeren Meinungsdifferenzen noch nicht in der kurzen Zeit diskutiert werden.
Ein weiteres großes Thema war: "Welche Serviceleistungen bieten wir an und warum?". Nun, der wohlbekannte und beliebte Prüfungsordner bleibt natürlich bestehen und wird laufend verbessert. Allerdings möchte ich an dieser Stelle gleich nochmals (ist ja schon wieder 6 Wochen her) betonen, daß wir nur dann am laufenden sein können, wenn Ihr uns neue Angaben bringt, schickt, in den Postkasten werft, o.ä. .Die Bibliothek wird derzeit auch neu organisiert, Beratungsfunktionen, wie u.a. Erstinskribentenberatung und Einführungstutorien für Erstsemestrige, sollen (inhaltlich) verbessert werden. Dazu gleich noch ein "Aufruf": Wir suchen interessierte und engagierte StudentInnen (Informatik, Datentechnik!) als Einführungstutoren für das kommende Wintersemester. (Masochisten aller Semester vereinigt euch!)
Weiters wurden Themen wie z.B.: Veranstaltungen, Anbieten Alternativer Lehrveranstaltungen, Arbeiskreise, Forschungsprojekte zu Randgebieten der Informatik, Vortragsreihe über das Berufsbild des Informatikers, verbesserte Kontakte zur HTU, Auslandskontakte u.v.m. diskutiert.
Das Fachschaftsseminar konnte in der Zeit nicht alle Bereiche der Fachschaftsarbeit behandeln, weitere (vor allem inhaltliche und politische) Diskussionen sind notwendig; trotzdem brachte dieses Seminar einige neue Ideen und Erkenntnisse, eine bessere Arbeitsaufteilung (in Ansätzen) und eine Menge Arbeit, um unsere Vorstellungen verwirklichen zu können.
Zum Abschluß: Jeder kann natürlich in das (wesentlich umfangreichere) Protokoll des Fachschaftsseminars Einblick nehmen. Anregungen, Wünsche und Beschwerden werden auch jederzeit in der Fachschaft entgegengenommen. (Fachschaftssitzung ist bekanntlich jeden Mittwoch um 16.00 Uhr).

Ed.

Computer-gestzützte Sauerei

Folgender Brief trudelte vor knapp einem Monat in der Fachschaft ein

Graz, am 27.4.1988

Basisgruppe Telematik
ÖH-TU GRAZ
Rechbauerstr. 12
A-8010 GRAZ

Liebe Kolleginnen und Kollegen !

Bei uns hat vor etwa einer Woche die erste Prüfung auf dem Computer stattgefunden. Es handelte sich dabei NICHT um einen Multiple-Choice Test, der nur mit dem Computer ausgewetet wurde. Es wurde im Gegensatz dazu verlangt, die Antworten direkt am Computer über die Tastatur einzugeben. Die Bedingungen entsprachen dabei nicht unseren WÜnschen. Zu Beginn der Prüfung waren die Fragen nicht bekannt, und beim Antworten über die Tastatur waren die Korrekturmöglichkeiten auf eine Zeile beschränkt, sobald diese abgeschlossen war, gab es kein zurück mehr. Zurückgehen war eigentlich gar nicht möglich, man konnte jede Frage nur einmal ansehen und sah auch nie mehr als die letzten 20 Zeilen seiner bisherigen Antwort. Die ganze Vorgengsweise ist also einerseits unheimlich (was passiert mit Leuten, die nicht Schreibmaschine schreiben können?), als auch rechtlich fragwürdig (AHStG Par. 23 Abs 1.).
Um die weitere Vorgehensweise koordinieren zu können und bessere Argumente dagegen zu finden, möchte ich euch bitten, mir eventuelle Erfahrungen mit diesem Problem als auch Vorschläge zu dessen Lösung zukommen zu lassen.

Vielen Dank im voraus

M. Brandl

(Manfred Brandl)

Das Problem an dieser Sache sehen wir eigentlich nicht in der schlechten Software, mit der die Prüfung abgehalten wurde, sondern im Modus der Durchführung. Das Gesetz (besagter § 23 Abs. 1 des AHStG) sieht folgende Modi für Prüfungen vor:

§ 23. Arten von Prüfungen

(1) Nach ihrer Methode sind folgende Prüfungen zu unterscheiden:
a) die mündliche Beantwortung der vom Prüfer gestellten Fragen (mündliche Prüfung);
b) die schriftliche Beantwortung solcher Fragen (schriftliche Prüfung);
c) praktische, künstlerische oder experimentelle Arbeiten, Konstruktionen oder schriftliche theoretische Arbeiten (Prüfungsarbeiten);
d) der Erfolg praktischer Tätigkeiten.

Daher sehen wir diese Computerprüfung als höchst illegal an. Außerdem stellt sie eine bedrohliche Entwicklung dar. Nicht nur, daß StudentInnen durch zusätzliche Aufgaben (Bedienung des Computers) belastet und abgelenkt werden, kommen plötzlich (rein theoretisch natürlich) völlig neue Dimensionen in der Beurteilung von Prüfungen hinzu: wie schnell hat StudentIn X diese Frage beantwortet, wie oft hat er/sie ausgebessert,... . Nicht mehr die Qualität der Antwort zählt dann, nein, eine völlig neue Qualität kommt dazu: lerne so, daß du die Antwort wie aus der Pistole geschossen parat hast. Das läuft einem vernünftigen Wissenserwerb völlig entgegen.
Außerdem kann durch den Computereinsatz eine völlig neue Variante von Prüfungsstreß erzeugt werden: zur Beantwortung dieser Aufgabe haben sie

35 Sekunden Zeit... . Es ist dann nicht mehr möglich, sich in eine Frage zu vertiefen, die man beherrscht, und dafür die zu vernachlässigen, bei denen man Schwierigkeiten hätte. Der Computer sorgt dafür, daß man über jede Aufgabe gleich wenig nachdenkt.
Weiters: wer garantiert, daß die/der StudentIn gerade diesen Editor beherrscht und gut damit umgehen kann? Wie sollen Angabefehler korrektiert werden, wenn andauernd Zeitstreß herrscht? Was ist, wenn ich pissen gehen will oder Dünnpfiff habe?
Es stehen heute in der Massenuniversität gewiß Probleme mit der Überprüfung des Wissen der StudentInnen an. Massenprüfungen sind da sicher keine gute Lösung. Doch die hier vorgeführte Variante stellt ganz sicher den Keller der möglichen Lösungsansätze dar. Sozusagen die unterste Schublade.

Leere Bibliotheks-regale

Das Schlagwort der Informationsüberflutung trifft für die neue TU - Bibliothek auch mit postmodernen Gestaltungsmerkmalen nicht zu. Insbesondere im Bereich der Informatik/Datenverarbeitung gähnt aus den Regallücken die Informationsdeflation. Auch wenn der/die BibliotheksbenützerIn nicht den Anspruch auf Aktualität erhebt, da ja bekanntlich ohnehin die durchschnittliche Halbwertszeit von Informatik - Sachbüchern bei einem dreiviertel Jahr liegt, wird er/sie auch auf der Suche nach "Klassikern" nur selten fündig, geschweige denn durch ein zufällig gefundenes Buch beglückt, das seinen/ihren Wissensdurst erst recht auslöst.
Eine Nachfrage in der Bibliotheksdirektion klärte die Ursache der Regalzwischenräume: Es gibt etwas Geld und auch Buchwünsche; ja viele neue Bücher sind sogar schon eingetroffen, nur ist das Personal derart überlastet, daß die Neuerscheinungen nicht den Weg vom Keller über die Karteierfassung in die Freihandbereiche finden. Bei der Planung der Bibliothek war ein EDV - System zur schnellen Datenerfassung projektiert, fiel aber - laut neuesten gerüchten nur zum Teil - dem Rotstift zum Opfer. Das Personal ist somit durch Karteiblättern und -ordnen und -suchen vollends ausgelastet.
Dennoch werden Literaturwünsche gerne entgegengenommen und bevorzugt behandelt. Gerade StudentInnen sollten diese Möglichkeit heftig beanspruchen, um die Palette der Literatur möglichst bunt zu halten, denn die Literaturvorschläge der Institute sind wohl oftmals sehr speziell und einfärbig. Entsprechende Formulare gibts beim Entlehnschalter.

Der österreichische Weg
oder: Aus dem Leben eines Studienplans

Marz '87	Seminar in Hernstein (NÖ), an dem StudentInnen (Egger, Schlemmer, Ratcliffe), Professoren (Barth, Kopetz, ...), Assistenten (Purgathofer, ...) und Sektionschef Höllinger vom Wissenschaftsministerium teil-nehmen. Zeugung des neuen Studienplans: Festlegung von Stunden-rahmen, Bedeutung von gesellschaftswissenschaftlichen Fächern.
April, Mai	Studienkommissionssitzungen, weitere Diskussion der Stundenpläne und Inhalte.
Juni	Beschluß des Wunsches nach einem neuen Studienplans durch die StuKo. GesamtStuKo mit Linz in Linz: Beschluß der Notwendigkeit zur Studienordnungsänderung. Fakultätskollegium beschließt Studienordnungsänderung und Wunsch auf Technikgesetzänderung (da Prüfungsfächer neue Namen erhalten und sich der Stundenrahmen ändert).
Ende Juni	Abgabe im Ministerium. Unwillige Annahme durch Höllinger, da eine große Technikgesetzänderung in Planung ist.
Jänner '88	Zusicherung durch Höllinger: Sofortige Aussendung des Entwurfs zur Begutachtung durch die Sozialpartner.
März	entgültige Aussendung, Ende der Begutachtungsfrist: Ende März.
3.Mai	Enquete: Einbringung von Änderungswünschen der Sozialpartner, Plan: bis 5.Mai sollen Änderungen fertig sein!
20. Mai	Änderungen sind fertig, Entwurf ist fertig zur Unterschrift durch den Minister, dann soll er ist Parlament. Ausdruck der Freude durch Höllinger über die Schnelligkeit des Verfahrens. Mündliche Garantie: Gesetzesänderungsantrag geht bis Mitte Juli ins Parlament, denn dann sind Ferien.
Zukunft	Höllinger legt Text Tuppy zur Unterschrift vor, so Tuppy will und kann, unterschreibt er und nimmt ihn in den nächsten Ministerrat zur Vorlage mit. dann ins Parlament, dann Bildung eines Ausschusses, dann Bildung eines Unterausschusses, dann 1. Lesung, dann 2. Lesung, Beschlußfassung, und das alles vor Mitte Juli!? (Who believes, gets sailing)

Trotzdem: keine Angst, es gibt im Herbst einen neuen Studienplan für die Informatik, ganz egal, ob das Parlament schnell genug ist oder nicht. Das betrifft aber nur die Erstsemestrigen.

Bericht von der 16.5 KIF in Aachen von 27.4.-1.5.1988

Die Konferenz der Informatikfachschaften (KIF) ist ein allsemesterliches Treffen von Informatikfachgschaftlern aus dem (erweiterten) deutschsprachigen Raum. Dort brüten die Teilnehmer in Arbeitskreisen über studentenpolitische, gesellschaftliche und universitäre Problembereiche. So findet ein internationaler Austausch von Erfahrungen in der Fachschaftsarbeit und der Studentenvertretung statt.

Folgende Arbeitskreise wurden dieses Mal angeboten:

Studienbedingungen, Studiendauer und Prüfungsbedingungen im Vergleich (FS Kiel)

Um gegen schlechte Studienbedingungen besser argumentieren zu können, wurde ein möglichst weitreichender Vergleich angestrebt.

Orientierungseinheiten und Erstsemestrigentutorien (Hannover)

Wie behandelt man Erstsemestrige gut, was soll ihnen geboten werden.

Studentenrechner (München)

An der TU-München gibt es den Plan, jeden Studenten zum Kauf eines Rechners zu zwingen, damit die Universität Geld spart. Was tun?

Neufassung des Datenschutzgesetzes in der BRD (Darmstadt)

Das DSG in Deutschland soll geändert werden. Welche Änderungen sind wünschenswert, wie kann man diese durchsetzen.

Einbettung wissensbasierter Systeme in die Umwelt (Karlsruhe)

AI in der "Wirklichkeit": kann das gutgehen?

Kreativ (TU Wien)

Computerkunst (TU Wien)

Wie beeinflußt der Computer den Künstler? Sind Computerstrukturen und Kreativität vereinbar?

Gesellschaftliche Auswirkungen der Informatik (Erlangen)

Dieses Jahr: erstellung einer relevanten Literaturliste zu diesem Thema

Projektstudium (Bremen)

Wie kann man eine weitere Akzeptanz des Projektstudiums durch die Lehrkräfte erreichen

Die 68er Studentenbewegung (?)

Welche Erfahrungen der 68er läßt sich heute verwerten.

Wieviel Liebe braucht die VAX (eigentlich: Wieviel Liebe braucht der Informatikstudent) (Zürich)

Kommunikationsschwierigkeiten bei Informatikstudenten - was tun?

Benutzerverhalten studentischer User an Terminals (?)

auf gut deutsch: Hacken

Bildung - was ist das? (?)

Prinzipielle Diskussion zur Bildungspolitik

Wir Wiener (Wäscherweiber...) waren mit 10 StudentInnen vertreten und haben auch zwei Arbeitskreise angeboten (s.o.)

Beim Schlußplenum wurden auch zwei Resolutionen beschlossen: eine zu Steffen Wernéry (siehe Titelstory) und eine zu den amerikanischen Cocom-Bestimmungen. Durch die kommt es in der BRD an einigen Universitäten zu konkreten Benachteiligungen von StudentInnen aus dem Ostblock. So dürfen zB. zwei Studenten aus der DDR nicht an die CRAY II in Stuttgart. Aus unserer Sicht bekommt diese Resolution eine eigentümliche Komik: Da auch für Österreich die Cocom-Bestimmungen tw. zutreffen, gibt es bei uns die bekannte "schwarze Liste" der Hi-Tech-Produkte, die nicht nach Österreich eingeführt werden dürfen.

PS: Auf die nächste KiF könnt ihr alle gratis; die ist nämlich an der TU in Wien!

Resolution der Konferenz der Informatikfachschaften

Durch die amerikanischen Cocom-Bestimmungen ist den Verkauf bzw. Weiterleitung von bestimmten High-Tech-Produkten (Supercomputer, ect.) an Länder, die den USA nicht "integer" erscheinen (Warschauer Pakt, Jugoslawien, tw. sogar Österreich, etc.) untersagt. Die Ausstattung von Universitäten mit davon betroffenen Geräten fürt in der BRD zu folgendem Problem: Studierende aus Ländern, die von den Cocom-Bestimmungen betroffen sind, kann die Benutzung dieser Geräte untersagt werden (also keine Rechnernummer etc.). Die KIF fordert die Universitäten daher auf, die Gleichstellung aller Studierenden unabhängig ihrer Herkunft zu gewährleisten oder gegebenenfalls die Anschaffung derartiger Geräte bis zu einer Änderung bzw. Aufhebung der Cocom-Bestimmungen aufzuschieben.

Themenschwerpunkt Computerkriminalität

Vor knapp einem halben Jahr hielt die Computerwelt den Atem an: Hackern war es gelungen, in etwa 135 Rechner, die an einem wissenschaftlichen Netz hängen, einzudringen und sich dort sämtliche Rechte zu verschaffen. Dieses Ereignis, daß sicherlich in die Geschichte der Informatik eingehen wird, führte in weiterer Folge zur Festnahme von Steffen Wernéry durch die französischen Sicherheitsorgane.
Wir bringen euch dazu auf den folgenden Seiten Hintergrund-material, soweit wir etwas auftreiben konnten. Da es sich dabei hauptsächlich um Material aus deutschen Mailboxen handelt, verzeiht bitte etwaige Satzfehler (ae statt ä, ss statt ß, ...). Außerdem drucken wir eine vierteilige Artikelserie der Washington Post überstzt ab sowie einige allgemeine Meldungen zum Thema "Computerkriminalität". Mehr Material zu diesen Themen liegt in der Fachschaft Informatik auf.

Peter Purgathofer

Inhalt

Greenpeace - außer Kontrolle, II

Eine Nachlese

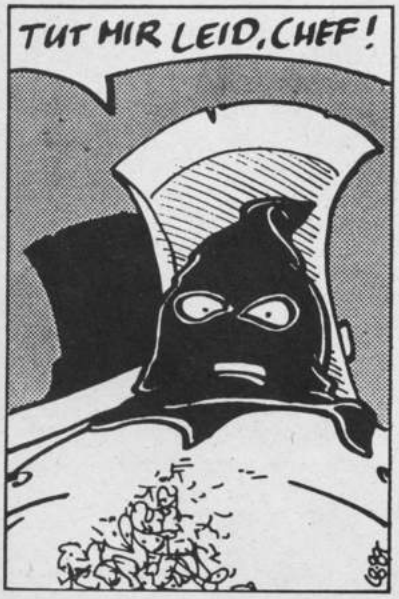
Etwa 1 Woche nach Erscheinen des fridolin 34 mit dem Artikel über die Außer-Kontrolle-Kleber (zur Erinnerung: diese trugen die Aufschrift "umweltfreundliche Polypropylenfolie" und waren aus PVC) erhielten wir einen empörten Anruf des Pressesprecher von Greenpeace-Österreich, Florian Faber.

- wären die Kleber aus Polypropylenfolie und nicht aus PVC, wie von uns behauptet, was auch ihre Chemikerin nachgewiesen hätte,
- die Grünfärbung des Beilsteintests, der eigentlich nur ein Vortest sei, käme von Chlorspuren im Kleber, ohne die es leider nicht ginge,
- sollten wir in Zukunft solche Stories sorgfältiger recherchieren, gerade als Technikerzeitschrift,
- gäbe es "lohnenswertere" Ziele als Greenpeace, die ja eigentlich gegen die Umweltverschmutzung arbeiten.

Er versprach weiters, einen Artikel bis zum nächsten Redaktionsschluß an uns zu senden, den wir selbstmurmelnd auch veröffentlicht hätten, wäre er nicht ausgeblieben.
Seine Seriosität stellte er gleich zu Beginn durch seine erste Frage ("Wer hat diesen Artikel geschrieben?") unter Beweis (Redaktionsgeheimnis!).
Sofort nach diesem Anruf haben wir eine eingehende Untersuchung des Klebers informell in die Wege geleitet (offiziell können wir uns das leider nicht leisten — ein Gutachten kostet öS 6000.-). **Sowohl unsere hauseigenen Chemiker als auch ein Kunststofflabor bestätigten uns, daß es sich bei diesem Kleber nicht um Polypropylen, sondern mit an Sicherheit grenzender Wahrscheinlichkeit um PVC handelt** ("Wenn das Polyprop ist, dann ist die Erde eine Scheibe!").
Daraus ziehen wir mehrere Schlüsse:
1. Offensichtlich ist die Greenpeace-Chemikerin nicht befragt worden, denn sie ist uns als seriöse Wissenschaftlerin bekannt.
2. Der **Vorstand** von Greenpeace-österreich legt ein Verhalten an den Tag, daß die **weltweite Bewegung** aufs **schwerste schädigt**. Denn wenn eine die Manager einer Umweltschutzorganisation nicht fähig sind, ihre eigenen Maßstäbe zu erfüllen, **dann sollten sie durch fähigere Leute ersetzt werden**. Alleine die Einstellung, daß es "angreifenswertere" Ziele als Greenpeace gibt, zeigt einen **sehr nachlässigen Umgang** mit der Idee dieser weltweiten Bewegung, **die ich als eine der treibenden Kräfte der internationalen Umweltpolitik** bezeichne!
Wir bitten hiermit Greenpeace erneut um eine offizielle Stellungnahme!

Der Nasa-hack

Unzureichendes Sicherheitsbewußtsein der Betreiber in Verbindung mit fehlender Aufklärung des Systemherstellers über einen die Integrität der Installation in Frage 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 Club (CCC) mehr als 135 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.

Grober Fehler im Betriebssystem

Die von dieser jungsten Hacker-Aktion betroffenen Rechner sind Systeme der VAX-Produktfamilie von DEC. In der ausgelieferten Version 4.4 des Betriebssystemes VMS (Stand Marz 1986) steckt ein Fehler, der die Integrität der Systeme erheblich tangiert. Das Betriebssystem stellt dem Benutzer einige hundert Systemaufrufe für Anwender-programme zur Verfügung. Das beschriebene Sicherheitsloch bezieht sich auf den Systemaufruf *SETUAI und erlaubt allen - also auch unberechtigten - Benutzern Schreibzugriffe auf die geschützte Datei SYSUAF.DAT. 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.

Privilegierter Rechnerzugang im SPAN

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) unabhangig davon, welche Privilegien für den benutzten Zugang gesetzt waren. Durch ein Maschinenprogramm wurden anschliessend mittels Systemaufruf und weiteren 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.

Trojanisches Pferd zum Kennwortsammeln

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 Hacker nun die so gesammelten Kennworte abrufen.

Trojanisches Pferd als Generalschlüssel

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 Überprufung 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 verwendeten 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.

Der automatische Hacker

Während ihrer über Monate andauernden Versuche gelang es der Hackergruppe schliesslich, diese Manipulationen weitgehend 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.

Das Sicherheitsloch - "groß genug für einen Schwertransporter"

Die fehlerhafte, im Mai 1986 ausgelieferte Version 4.4 des VMS-Betriebssystems wurde im Dezember 1986 durch die Version 4.5 ersetzt, die die gleichen fehlerhaften Mechanismen erhielt. 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 Sicherheitsprogrammes an. Bei Nichtbeachtung könne, so die Ankündigung zu dem Programm, die Integrität des Systems Schaden nehmen.

Beim Spielen ins Softwareloch gefallen

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 Sicherungsprogrammes. 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.

Manipulation von Systemmanager entdeckt

Durch Zufall gelangte ein Systemmanager in den Besitz der Hackerprogramme. Er veranlaßte Kollegen auf einer VAX, welche in einer Datei über Netzwerkverbindungen protokolliert war, alle Benutzerdateien nach den Hackerprogrammen abzusuchen. Mehrere Tage wurden die so entdeckten Programme untersucht, bis nach und nach die Möglichkeiten des Trojanischen Pferdes erkannt wurden. Daraufhin versandte der Systemmanager Anfang August 1987 Warnungen an fast alle Netze und diverse Verteiler.

Im Spannungsfeld des Know-how-Transfer

Den Hackern genügte es nach ihren Angaben, die Rechner nur zu öffnen und die Schwächen der Systeme aufzudecken und nachzuvollziehen. Weitere Ziele wurden nach eigenem Bekunden nicht verfolgt. Obwohl hin und wieder in den Datenbeständen gewühlt wurde, hatten die Hacker kein prinzipielles Interesse an den Inhalten der betroffenen Systeme. Durch die über Datennetze verbreiteten Warnungen des Systemmanagers ergab sich jedoch eine Situation, die für die Hacker nicht mehr kalkulierbar erschien. Denn nun wäre es jedem gut Informierten möglich gewesen, seinerseits das Generalkennwort an anderen - möglicherweise betroffenen - Systemen auszuprobieren, ja vielleicht sogar das ganze Vorgehen nachzuvollziehen. Dieses Wissen in falschen Händen befürchten zu müssen, gab Anlaß zu Besorgnis: Die Hacker fanden sich plötzlich im Spannungsfeld von Industriespionage, Wirtschaftskriminalitat, Ost-West-Konflikt, COCOM-Embargo und legitimen Sicherheitsinteressen von High-Tech-Firmen und -Institutionen -- sie zogen die Notbremse.

Maßnahmen zur Schadensbegrenzung

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 Schaden und mögliche Gefährdungen der Integritat 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 militarischen Forschung um verantwortliche Darstellung und Vermittlung.

Chaos Computer Club e.V.

Die Folgen

Fahndungsdruck wird erhöht

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

Mitte September trat der Club mit Informationen an die Öffentlichkeit, die ein eklatantes Sicherheitsloch in einem Großrechnerbetriebssystem der Firma Digital Equipment belegten. "Hacker" hatten sich an den Club gewandt, nachdem es ihnen gelang in circa 135 Computersysteme des wissenschaftlichen Informationsnetzes der Luft- und Raumfahrt sowie der Hochenergiephysik einzudringen.

Mittels sogenannter "Trojanischer Pferde" untergruben sie die Sicherheitsroutinen und installierten unter anderem Programme, die die Kennworte aller Nutzer auskundschafteten. Betroffen von diesem "Hack" waren neben der amerikanischen Raumfahrbehörde NASA führende Institute im neun westlichen Ländern.

Bei der durch den Club sofort nach Bekanntwerden eingeleiteten "Schadensbegrenzung" wurde neben dem Hersteller auch der amerikanische Geheimdienst CIA informiert. Man wollte, so ein Clubsprecher, vermeiden, dass der Club sich aufgrund der Brisanz der betroffenen Systeme zum Spielball der Geheimdienste entwickelt. So war es selbstverständlich, dass vor einer Veröffentlichung die betroffenen Systeme wieder "gesichert" werden mußten.

Beim Vergleich der von den "Hackern" angefertigten Liste der betroffenen Computer mit der Liste des Herstellers ergaben sich jedoch zahlreiche Unstimmigkeiten. So wurden an führenden Forschungseinrichtungen, auch im Bundesgebiet, auf dem second hand Markt erworbene Grossrechner ohne Lizenz betrieben. Gemeinhin wird soetwas als "Raubkopie" bezeichnet.

Als Folge der Veröffentlichung dieses "Hacks" besannen sich die Wiesbadener Polizeispezialisten einer Anzeige der französichen Niederlassung der Philips AG. Diese hatte im Herbst 1986 - nachdem der Gesetztgeber in der Bundesrepublick das Ausspähen und Verändern von Daten unter Strafe stellte - Anzeige erstattet. Nach Angaben von Philips waren Hacker in die Fertigungssteuerung eingedrungen.

Die Ermittlungen der französischen Behörden führten in die Schweiz zum Genfer Kernforschungszentrum CERN. Dieses beklagt schon seit 1984 ständig Einbrüche durch Hacker. Unter den Hackern selbst gilt CERN als die "Europäische Hackerfahrschule" in der sich die Hacker "die Klinke in die Hand geben". Die schweizer Systemspezialisten äusserten den Ermittlungsbehörden gegenüber den Verdacht, daß der Hamburger Chaos Computer Club Verursacher dieser Einbrüche sei.

So erwirkte die Staatsanwaltschaft, einen Tag nach Veröffentlichung des Nasa-Hacks, die ersten Durchsuchungsbeschlüsse. Inzwischen wird gegen sieben "Computerfreaks" aus dem Umfeld des CCC, inzwischen auch wegen des publzierten NASA-Hacks, ermittelt. Begleitet wurden die Ermittlungen durch ebensoviele Hausdurchsuchungen, bei denen umfangreiches Material sichergestellt wurde.

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

Seit der letzten Durchsuchung sind knapp vier Monate vergangen. Bis zum heutigem Tage wird den Anwälten der Beschuldigten die Akteneinsicht verwehrt. Das BKA und die Staatsanwaltschaft tun sich schwer Licht in das Dunkel dieses Falles zu bringen. Mag auch das sichergestellte Material an Umfang zwar zugenommen haben, so scheinen die Spezialisten vom BKA nicht in der Lage zu sein ihre Vorwürfe zu präzisieren und zu belegen.

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

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

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

Steffen Wenréry

CCC ev
Schwenckestr. 85
D-2000 HH 20

Philips France
Data Security Manager
50, Avenue Montaigne
F 75380 Paris
00331-42568800

Hamburg, den 17. Feb 1988

Betr.: SECURICOM 1988 in Paris Bezug: Ihre Strafanzeige vom August 1986

Sehr geehrte Damen und Herren,

wie wir erst kürzlich aus einem Gespräch im Bundeskriminalamt erfuhren, wurde im August 1986 eine Anzeige von der französischen Niederlassung der PHILIPS gegen den Hamburger Chaos Computer Club e.V. erwirkt.
Dieses hatte zur Folge, dass im September 1987 über 25 Beamte deutscher und französischer Stellen die Wohn- und Geschäftsräume der Vorstandsmitglieder des CCC durchsuchten.

Leider ist uns bis zum heutigen Tage unklar, welche Ereignisse hinter der Strafanzeige stehen.

Da ein Vertreter des CCC am 15. März 1988 auf der SECURICOM in Paris Stellung zu diesem Sachverhalt nehmen wird, stellt sich für uns die Frage, ob sie im Vorfeld an einem vertraulichen Gespräch mit uns interessiert sind. Als Termin käme der 14. März in Frage. Leider an diesem Tage nur am Nachmittag, da am Abend bereits ein Gespräch mit dem Programmkommittee angesetzt ist, in dem auch das Pressemanagement der SECURICOM erörtert wird.

Mit freundlichen Grüssen
Wau Holland
Steffen Wernery

Französischer Geheimdienst gegen Hacker

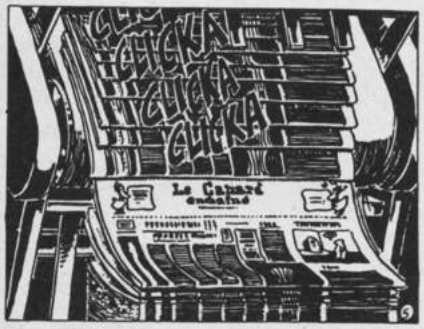
Wie das deutsche Konsulat in Paris mitteilte, wurde das Vorstandsmitglied des Chaos Computer Club, Steffen Werneéry, bei der Einreise zum 6. Weltkongress zu Datenschutz und Kommunikationssicherheit (SECURICOM '88) in Paris von der französischen Polizei verhaftet. Steffen Werneéry ist einer der Referenten für die SECURICOM. Das seit Monaten angekündigte Thema für die Eröffnungsveranstaltung am 15. März sind Hintergründe des bekannten NASA-Hacks vom Herbst 1987. Bis jetzt war keine Stellungnahme des Ausäwrtigen Amtes zu erhalten. Die französische Polizei ist, wie das deutsche Konsulat in Paris mitteilte, nicht zu Auskünften verpflichtet.

Hamburg/Paris (lno) - Das Vorstandsmitglied Steffen Werneéry wurde am Montag Nachmittag von französischen Beamten verhaftet. Dies bestätigte Wernérys Anwalt Axel Bauer gegenüber der Deutschen Presse-Agentur (DPA). Werneéry hielt sich anlässlich des 6. Weltkongress zu Datenschutz- und Kommunikationssicherheit, SECURICOM 88, in Paris auf. Er war zur Eröffnungsveranstaltung als Referent zum Thema Datensicherheit eingeladen. Zur Stunde ist unbekannt, warum Werneéry verhaftet wurde. Wie das Deutsche Konsulat in Frankreich mitteilte, sei die französische Polizei nicht verpflichtet Auskunft zu erteilen. Hintergrund der Verhaftung sind, nach Angaben des Chaos Computer Clubs, vermeintliche Hackeraktivitäten in französischen Großrechnern der Firma Philips. Die französische Niederlassung der Firma Phillips hatte Wernery anläßlich der SECURICOM zu einem ersten Hintergrundgespräch eingela-den. Das Gespräch mit den Philips-Managern konnte nicht stattfinden, da Wernery verhaftet wurde. Wie dem CCC mitgeteilt wurde, verhören die französischen Behörden zur Stunde auch den Herausgeber der in Pullheim bei Köln erscheinenden Zeitschrift "Der Datenschutzberater", Hans Gliss. Gliss war ebenfalls als Teilneher der Eröffnungsveranstal-tung eingeladen. Die Veranstalter der SECURICOM haben sich über die "dubiosen Vorgänge" der Verhaftung "äusserst ungehalten gezeigt".

Presse-spiegel

Die internationale Presse der ersten Tage

Paris(taz) - Steffen Wernéry soll in Paris der Prozess gemacht werden. Der Hamburger Vize-Vorsitzende des Hamburger Chaos-Computer-Clubs, der am Montag überraschend in Frankreich festgenommen wurde, soll nach Auskunft seiner Anwältin zumindest wegen Anstiftung zur Hackerei unter Anklage gestellt werden. Untersuchungsrichter Fontanaud bestätigte abends die Fortsetzung der Verhöre. Zuvor war Wernéry, dem offenbar Hackversuche gegen die französische Philips-Filiale und der französischen Weltraumbehörde (CNES) vorgeworfen wird, 48 Stunden lang von der für Informatikvergehen spezialisierten Pariser Finanzpolizei vernommen worden. Polizeichef Lacoste bestätigte der taz, daß Wernery nicht etwa als Zeuge sondern als Tatverdächtiger einsitzen muß. Lacoste berief sich auf Razzien, die seine Polizei mit bundesdeutschen Kollegen 1987 in der Wohnung Wernérys durchgeführt hatten.
(Fortsetzung Seite 2, u.l.)
In Paris, so Lacoste, habe man nur auf den Besuch Wernérys gewartet, da er in der Bundesrepublik alle Aussagen verweigert hätte. Wernery hatte bisher behauptet, dass er von der Affäre, innerhalb der er verdächtigt wird, erst mit den damaligen Untersuchungen der Polizei erfahren hatte. Anders als in der Bundesrepublik, wo Hacker-Eingriffe nur bei entstehnden Schäden strafbar sind, kann sich die französische Polizei bei ihrem Vorgehen heute auf ein Gesetz vom 5. Januar dieses Jahres berufen, nachdem "jeder, der sich auf betrügerischem Wege Zugang in ein automatisches Datensystem verschafft, mit einer Haftstrafe von zwei Monaten bis zu einem Jahr oder einer Geldstrafe von 2.000 bis 50.000 Francs bestraft" werden kann. Mit anderen Worten : jeder Hack-Versuch ist strafbar.



Assotiated Press
15 Mar 88 West German Chaos Computer Club official WERNÉRY held by French police in connection with hacking operation (335)
PARIS Police have arrested an official of a West German hacker club in connection with the infiltration of sensitive French computers as he arrived in France for a convention on computer security, informed sources said Tuesday. Steffen WERNÉRY, 26, board member of the Hamburg-based Chaos Computer Club, was detained Monday for questioning by police of the Financial Brigade on his arrival at Orly airport, according to the sources.
Examining Magistrate Daniel Fontanaud, charged with investigating computer pirating among French companies, on Tuesday extended the period of detention for 24 more hours, until Wednesday, the sources said.
Chaos Computer Club gained attention last year with the infiltration by some club members and other hackers of NASA-SPAnet, a network connecting scientific research centers. Some NASA computers as well as computers of the Geneva-based European Institute for Nuclear Research and France's National Center for Space Studies were infiltrated. After the scandal broke in September, US officials denied the hackers' claims that they had accessed a sensitive NASA computer, saying there was nothing highly classified in the information banks used by researchers worldwide that were accessed.
According to the French news agency Agence France-Presse, quoting well informed sources, WERNÉRY 'did not deny pirating' French computers but told police 'he was not alone and implicated others.'
WERNÉRY came to France for the three-day convention of SECURICOM. He was reportedly to present a paper on the infiltration of the NASA-SPAnet system. 'It is a pity that such an important convention guest is being held by police before he can even explain himself in public,' SECURICOM director Peter Hazelzet is quoted as saying. Hazelzet said the SECURICOM convention is considered the most important in the field of computer security and was the first to reveal, two years ago, the existance of 'computer viruses,' the destruction of computer programs, according to AFP.

PARIS (Reuter) - Computer experts say a 19-year-old West German hacker has succeeded in breaking into one of the world's top-selling computers, Digital Equipment Corp.'s VAX system. Experts called the action a blow to confidence in computer security. Computer specialists broke the news this week at a computer conference already shocked by the arrest Sunday of hacker Steffen Wernéry, who was apprehended as he arrived to take part in a debate on system security. Wernéry is a member of the Hamburg-based Chaos Computer Club, which caused a storm last year when it revealed it had penetrated more than 100 computers around the world, including the network of the U.S. space agency, NASA. French police said later that Wernéry had been charged with "theft, destruction and damaging computer goods" and had been jailed pending trial. Hans Gliss, a West German journalist and computer expert who was also held briefly by French police when he arrived in Paris, said the unidentified 19-year-old from Munich had worked out how to enter VAX computers made by Digital. Gliss said the Munich hacker had breached the VAX system by using material available from Digital. Digital executives were not available for comment. Rudiger Dierstein, who is with West Germany's national space foundation, said the hacker's achievement had terrifying consequences for privacy. West German and French police raided the club's offices after the revelations.

Reaktionen

Der Chaos Computer Club erklärt zur Festnahme seines Vorsitzenden Steffen Wernéry am 14. März 1988 durch französische Behörden:

Der Journalist und Systemberater Steffen Wernéry, wurde von den Veranstaltern der SECURICOM in die Hauptstadt der Republik Frankreich eingeladen um dort vor internationalem Fachpublikum über Probleme der Computersicherheit zu referieren. Ausserdem war er vom CCC beauftragt, klärende Gespräche mit der Firma Philips zu führen. Gegenstand des Vortrages sollte unter anderem auch der spektakuläre NASA - Hack sein, bei dem der Chaos Computer Club als Vermittler zwischen nicht genannten Hackern und den Behörden tätig gewesen ist.

Der Chaos Computer Club hat in der Vergangenheit immer wieder darauf aufmerksam gemacht, dass Fragen der Systemsicherheit und Kommunikationssicherheit von Herstellern und Anwendern oft grob fahrlässig gehandhabt werden. Der CCC hat alles versucht, um die Entstehung größerer Schäden abzuwenden.

Bei den Vermittlungstätigkeiten wurde bereits am 15.August 1987 der bundesdeutsche Verfassungschutz eingeschaltet, um den verantwortlichen Computerhersteller DEC von offizieller Stelle aus zu informieren und die betroffenen Systembetreiber in die Lage zu versetzen, rechtzeitig zu handeln.

Der CCC protestiert auf das Schärfste gegen das Vorgehen der französischen Ermittlungsbehörden. Damit haben die Verantwortlichen dazu beigetragen, daß dem internationalen Fachpublikum erhebliche Systemmängel auch in französischen Computeranlagen nicht erläutert werden konnten.

Zudem ist die offene Diskussion und in der Folge, sachdienliche Schadensbegrenzung, verhindert worden.

Es sollte auch den französischen Behörden bekannt sein, daß der CCC in der BRD eine wichtige Rolle in der Diskussion um Probleme der Informationsgesellschaft hat.

Der CCC betrachtet das Vorgehen gegen sein Vorstandsmitglied als eine erhebliche Beeinträchtigung journalistischer Arbeit. Angesichts der Vorfälle in Paris stellt sich dem CCC die Frage, was einem Journalisten zu raten ist, wenn er mit brisanten Informationen nach Frankreich einreisen will.

Der CCC war bis zu den jüngsten Ereignissen stets zu offenen und öffentlichen Gesprächen bereit. Das Vorgehen der französischen Behörden ist dieser Dialogbereitschaft abträglich.

Der CCC fordert die französischen Behörden auf, unverzüglich bekanntzugeben, was Wernéry vorgeworfen wird. Wernéry wird nunmehr bereits seit mehr als 48 Stunden ohne rechtskräftigen Beschluß in Gewahrsam gehalten. Der CCC protestiert entschieden gegen diese Willkürmaßnahme. Er hat heute offiziell das deutsche Konsulat in Paris und die Bundesregierung um Hilfe ersucht.

gez. Reinhard Schrutzki / Herwart Holland-Moritz

Restvorstand des Chaos Computer Club e.V.

bonn, 15.03.88
pressemitteilung nr. 272/88

grüne fordern sofortige freilassung von steffen wernery

anlässlich der verhaftung des vorstandsmitgliedes des hamburger chaos computer clubs (ccc) steffen wernéry in paris schickte regula bott, fraktionssprecherin der grünen im bundestag, das folgende protesttelegramm an das französische innenministerium und die französische botschaft in bonn:

'ich protestiere gegen die verhaftung steffen wernéry's. wernéry befand sich auf einladung des philips konzerns in frankreich. verhaftet wurde er aufgrund einer strafanzeige eben dieses konzerns. die mysteriösen umstände von wernery's verhaftung sowie die tatsache, dass die französischen staatsschutzbehörden bis zum jetzigen zeitpunkt sich weigern, den derzeitigen aufenthaltsort des verhafteten bekannt zu geben, sprechen jeder rechtsstaatlichkeit hohn.

ich fordere die unverzügliche freilassung steffen wernéry's.'

Resolution der Konferenz der Informatikfachschaften

Seit Mitte März wird Steffen Wernéry vom CCC im Gefängnis Paris-Frenet ohne Grundlage festgehalten. Wir sehen in dieser Maßnahme der französischen Justiz einen Einschüchterungsversuch gegen bewußte Informatiker wie etwa die Mitarbeiter des CCC und verurteilen die Inhaftierung daher als Machtmißbrauch und Verletzung der Menschenwürde.

Wir fordern die sofortige Freilassung Steffen Wernérys!

Aachen, den 30. April 1988

Hintergründe

Ein Artikel aus der Disksussion um den CCC

Seit 1984 führt der CCC eine konstruktive Diskussion zu den seit 1986 geltenden Wirtschaftskriminalitäts-Gesetzen, in die auch Delikte der Computerkriminalität aufgenommen wurden. Nach Auffassung des CCC, sind diese Gesetze offensichtlich nicht geeignet, den Problemen der Computerkriminalität differenziert und wirksam zu begegnen. Technische Fehler können nicht mit Gesetzen behoben werden! Genausowenig können Gesetze mangelndes Verantwortungsbewusstsein ersetzen. Die Praxis zeigt jetzt, das diese Gesetze gegen jene angewendet werden, die dazu beitragen, das Problembewustsein zu schärfen.

Schon bei den Beratungen der neuen Gesetzgebung hatte beispielsweise Prof. Dr. Ulrich Sieber, als internationaler Experte für Computerrecht, dem Bundestag vorgeschlagen, Hackern bei Selbstanzeige und Aufdeckung aller Umstände Straffreiheit zuzusichern. Im Steuerrecht ist diese Straffreiheit bei Selbstanzeige bereits verwirklicht. Damit wäre ein Weg eröffnet, das Wissen der Hackerszene in einen konstruktiven und gesellschaftlich nützlichen Dialog einfliessen zu lassen.

In seinem Schreiben an die Clubmitglieder erklärte Werneéry: "Wir haben verantwortungsvoll gehandelt - auch wenn es bei der unbedachten Gesetzgebung schwer ist. Wir sollten diese Linie nicht verlassen".

Im Zusammenhang mit Wernerys Verhaftung in Paris, will der französische Untersuchungsrichter Daniel Fontaneaud jetzt auch Vorstandsmitglied Wau Holland vernehmen. Ein entsprechendes Ansinnen wurde über die Pariser Anwältin Eva Sterzing an Holland übermittelt. Dazu soll Holland nach Paris reisen.

Wau Holland erklärte, er habe bereits anläßlich der Durchsuchungen im November gegenüber deutschen und französischen Ermittlungsbeamten ausgesagt. Er sei weiterhin bereit, dies zu tun. Allerdings könne man von ihm nicht ernsthaft erwarten, daß er, wie gewünscht, zur Vernehmung nach Frankreich kommt. Holland schlug vor, sich auf neutralem Boden zu treffen. Zeitpunkt und Ort dieses Treffens müsse deutschen und französischen Medien bekanntgegeben werden.

Holland erklärte am Montag gegenüber der Presse, er habe im Juni einen ohne Absender verschickten Briefumschlag erhalten, in dem sich ein fingerdicker Stapel mit Unterlagen zum NASA-Hack befanden. Nachdem das Material gesichtet war, wurde im kleinen Kreis umgehend beschlossen, Hersteller, Betreiber und deutsche Sicherheitsbehörden zu informieren. Gleichzeitig recherchierte ein dpa-Journalist, der durch die Nachricht eines besorgten Systemmanagers auf die Geschichte aufmerksam wurde.

Am 15.8.1987 wurde zwischen einem Vertreter deutscher Sicherheitsbehörden und den CCC-Vorstandsmitgliedern Steffen Werneéry und Wau Holland ein Informationsgespräch geführt. Zum Beweis der vom CCC aufgestellten Behauptungen, wurde eine Liste von 135 betroffenen Rechnersystemen, eine Dokumentation der Manipulationsmethode und die dazu benutzten Programme vorgelegt. Die Behörden wurden gebeten, ihre Möglichkeiten der Schadensminimierung zu nutzen. Es bleibt festzustellen, daß der Computer-Hersteller die Informationen erst glaubte, als dpa und Panorama am 15. September 87 über den sogenannten NASA-Hack berichteten.

Wie Frank Berger, Geschäftsführer für den Bereich Unternehmenskommunikation bei Digital Equipment Corporation (DEC), anläßlich einer Podiumsdiskussion auf der diesjährigen Computer-Messe CEBIT in Hannover erklärte, habe der Vergleich zwischen der "Hackerliste" betroffener Institutionen und der DEC Kundenwartungsliste ergeben, dass einige Institutionen Raubkopien der Betriebssystem-Programme verwendeten. DEC habe jedoch keinen Strafantrag gestellt, um das Geschäftsverhältnis nicht zu belasten. Es wurden lediglich Verwarnungen ausgesprochen.

Es ist festzustellen, daß der Chaos Computer Club von sich aus auf Sicherheitsbehörden zugegangen ist und diese im Rahmen seiner Möglichkeiten umfassend informiert hat. Anstatt sich nun unverzüglich um die Schadensminimierung zu bemühen, wurde unter anderem von Philips Frankreich eine "Hacker- und Häcksenjagd" eröffnet, die von der Hamburger Staatsanwaltschaft und vom Bundeskriminalamt ausgeführt wurde. In diesem Zusammenhang ist nicht mit Sicherheit auszuschliessen, daß das am 24. März 1988 von der Illustrierten STERN veröffentlichte Password noch immer den unberechtigten Zugriff auf Systeme erlaubt.

Aufklärung muß hier betrieben werden, aber auch das politische Gespräch mit allen Erreichbaren ist unerlässlich. Es ist zu erwarten, daß in der Zukunft restriktive Gesetzgebungen im Bereich Datenkommunikation vom Zeitgeist überholt sein werden. Das Wandern auf den Netzen wird zum allgemeinen Wissensquell. Öffentliche Datenbanken mit allen relevanten Informationen werden dann zur Verfügung stehen. Das Recht auf Kommunikation für jedermann wird Strukturen verändern. Das Schlagwort "Wissen ist Macht" wird der Wahrheit "Wissen ist frei" weichen. Die Arbeit von Steffen Werneéry ist in diesem Zusammenhang zu sehen. Das hat nichts zu tun mit den Sensationslüsten einiger Beteiligter. Der Mut von Wernery und anderen Clubmitgliedern darf nicht gleichgesetzt werden mit krimineller Energie. Die Menschen haben ein Recht darauf, nicht immer angepaßt zu denken. Gerade von solchen Geistern gehen die entscheidende Impulse aus.

Hacks aus aller Welt

Hacker runs rings round military security

A West German has shown how easy it is to break into sensitive military and university files in other countries, using a computer and a modem. From his base in Hanover, the computer "hacker" spent two years breaking into more than 30 computers at military bases, defence contractors and universities in the US, Japan, West Germany and Canada. His motive is still unclear, altough some people allege it was espionage. Most of the files that he entered dealt with military matters. He obtained no classified information, says the US Dep. of Defence. But computer experts familiar with the case say that the files, when added together, would have been useful to a spy. The files included summaries of the US Army's plans for nuclear, biological, and chemical warfare in central Europe. An elaborate "sting" operation, centered at the Lawrence Berkeley Lab (LBL) in California, took eight months to snare the hacker. The operation caught him only when he stayed on "the system" much longer than usual, after he had been led into a bogus file on SDI. The hacker saw but ignored elaborate games that had been set up to trap him. "This suggests that what he was doing was not a hobby", Clifford Stoll from LBL said last week. Investigators say the hacker used the name Mathias Speer. He appears to be a computer science student at a German university. Both the FBI in the US and its German equivalent, the BKA, are investigating the case, but neither has yet laid charges. Speer may not be liable for prosecution under existing German law. In California, he would be liable to pay $100000, the cost of computer time spent tracking him down. Speer has been linked to an American businessman who reportedly acts as a broker for deals in weapons with Saudi Arabia. He denies knowing Speer, but was implicated when he sent a letter to LBL in California asking about a file that was, say the investigators, known only to the hacker. Stoll, an astronomer at LBL who set the trap for the hacker, said last week that the case showed the laxity of computer security. [.....] Stoll described the intruder as plodding and methodical, but not a wizard. He tried to enter about 450 computers, and was first detected at LBL in late 1986, when he created a new account and used it to break into Milnet. This is an unclassified communications network that links military bases with contractors working for the DoD. He also used LBL to connect to Arpanet, another unclassified military computer network. The hacker made most of the connections to the military computers via Arpanet and Milnet. Investigators traced the intrusion to a defence contractor in McLean, Virginias, and from there to university computers in Bremen and Karlsruhe. The hacker used a lokal telephone call to reach the universities computers. He persuaded those computers to give him the status of a system manager, so bypassing the normal accounting procedures, and used the university computers to make connections overseas via the German digital network called Datex-P. Stoll said the episode showed how vulnerable businesses could be to industrial sabotage by computer. A competitor could break into a business computer to read, delete or alter data, he said. The West German intruder entered a computer that controlled medical experiments. "He could have injured patients either deliberately or unwittingly. It shows how dangerous this can be," Stoll said. The intruder was identified in August last year. LBL released details of the sting operation last week. Next week, Stoll's account of what happened - and how similar incidents can be prevented - will be published in Communications of the ACM.

Ian Anderson / New Scientist

dpa-Eurodienst <18.7.1986>

Paris (dpa) - Ein "Hacker" hat in Frankreich einen Supercomputer angezapft, in dem geheime Informationen aus Rüstung und Forschung gespeichert sind. Wie die französische "Le Matin" am Freitag berichtete, ereignete sich Vorfall am Osterwochende in der Nacht vom 30. zum 31. März. Der Eindringling konnte bisher ebensowenig identifiziert werden, wie die Mittel, mit denen er sich Zugang, zu den aus den USA stammenden Computersystem im Wert von 10 Millionen Dollar verschafft hatte. Es gilt als eines der sichersten der Welt.
Nach dem Bericht wird der Computer "CRAY ONE", der in der Eliteschule Polytechnque aufgestellt ist unter anderem von der Rüstungsabteilung des Verteidigungsministeriums vom Nationalen Amt für Raum- und Luftfahrtforschung (Onera) und vom Forschungszentrum CNRS benutzt. Der "Hacker" habe mehrere Stunden lang den Speicher eines ihm vorgeschalteten Elektronengehirns durchsucht, hiess es. Offen sei aber, ob der Eindringling über eines der geheimen Schlüsselworte in dem Computer kam oder es mit eigenen Mitteln geschafft habe. Inzwischen wurde Klage gegen unbekannt erhoben.

Nachlese zum NASA-Hack

1. Softwareklau - auch bei Grossanwendern

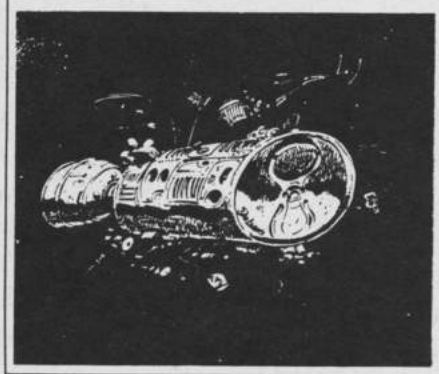
Wer eine Spielesoftware für Homecomputer kopiert, hat Software gemaust. Schlechtes Gewissen? Vielleicht ein bisschen. Wer ein ganzes Betriebssystem auf ähnliche Weise besorgt, hat dem eigenen Laden viel Geld gespart. Darauf ist man stolz.

Die NASA-Hacker brachten es an den Tag. Eine Liste mit 135 infizierten Rechnern waren mit Hilfe von Steffen Wernery und des Datenschutzberaters aus dem Kreis der Täter an Deutsche Sicherheitsbehörden und von dort aus an den betroffenen Hersteller, DEC, gelangt. Die Hacker hatten noch verwundert angemerkt, bei einigen Rechnern, bei denen sie es versucht hatten, seien ihre eigenen Betriebssystemveränderungen unerklärlicherweise schon drin gewesen.

DEC fand rasch die Erklärung: Auf Anlagen, die vom Second Hand Markt beschafft waren, hatten die Betreiber des Betriebssystem VMS in einer bei Kollegen "organisierten" Kopie gespielt. Ein sonst gut beleumundetes Europäisches Forschungsinstitut hatte es gar toll getrieben: In Deutschland liefen drei VAXen, davon waren aber nur eine und das dazugehörige Betriebssystem bei DEC gekauft. Die Hacker konnten zwischen lizensierter Software und Raubkopie nicht unterscheiden - sie infizierten alle drei.

Auf einer CeBIT-Podiumsdiskussion erläuterte DEC-Geschäftsführer Frank Berger den Sachverhalt und erklärte, dass bislang gegen betroffene Universitäten und Forschungseinrichtugen kein Strafantrag gestellt wurden. DEC habe lediglich "Verwarnungen" ausgesprochen.

2. Neue Vorfälle aus der Hacker-Szene



Nach wie vor werden VAX-Anlagen von unbefugten Benutzern attakiert. Dem Datenschutz-Berater liegen hierzu unterschiedliche Informationen, auch aus Deutschland, vor; teilweise auch unmittelbare Erkenntnisse der französischen Polizei, denn dies war Gegenstand von Ermittlungen, in die der Datenschuzt-Berater involviert war. Nachdem im Februar der Redaktion vertraulich von neuerlichen Penetrationsversuchen in der Bundesrepublik berichtet wurde, und nachdem am 24. Februar 1988 in einer britischen Mailbox Spekulationen über erneute Angriffe des SPANnet veröffentlicht wurden, recherchierte der Datenschutz-Berater, was es damit auf sich haben könnte. Die für den NASA-Hack Verantwortlichen wurden unter Wahrung der Anonymität über den CCC befragt, ob sie was wüssten. Die Antwort lautete:

Man habe neürlich nichts unternommen, von einer Ausnahme abgesehen, die ein positives Ziel hatte. Nach Veröffentlichung des NASA-Story habe man sich über die Reaktion der NASA gewundert. Ein Sprecher der NASA hatte öffentlich verkündet, die Sache sei keine reale Bedrohung der Rechnersicherheit gewesen; man habe ohnehin nur Daten gespeichert, die allen Wissenschaftlern so frei zugänglich seien wie Daten in einer öffentlichen Bibliothek.

Daß zwischen einem derartigen Zugriff auf wissenschaftliche Daten und den Rechten, die sich die Hacker eingeräumt hatten (eben Änderungen im Betriebssystem) ein wesentlicher Unterschied besteht, wurde vom NASA- Sprecher offenbar zu Kenntnis genommen.

Daraufhin hätten die Hacker gegen Ende September einmal nachgeschaut, ob die NASA-Rechner inzwischen dicht seien; ein Computer war in der Tat noch offen. Nun habe man aus "eigenem Verantwortungsgefühl" gehandelt, hiess es. Man habe von Deutschland aus die notwendigen Modifikationen des Betriebssystems vorgenommen, um den NASA-Rechner dicht zu machen gegenüber Hackern.

Diese Geschichte ist insoweit glaubhaft, als sei einerseits Spekulationen über neueliche Hackeraktionen im SPAN-Net erklärt, andererseits passt sie ins Bild, wei die deutschen Hacker bekanntnlich kalte Füsse bekommen hatten, nachdem Anfang August 1987 jemand im Netz Hinweise auf ihre Verfahren veröffentlicht und damit einer unbekannten Zahl von Systembenutzern den Weg für erfolgreiches Hacking gewiesen hatte.

<aus:Datenschutzberater 4/88>

Aktuelles zum Fall Werneéry

Die neuesten verfügbaren Meldungen

Französische Behörden lassen sich Zeit

Hamburg (jwi) - Seit nunmehr 52 Tagen wird Steffen Wernery, Vorstandsmitglied des Hamburger Chaos Computer Clubs (CCC) in französischer Untersuchungshaft festgehalten. Nach wie vor gibt es keine konkreten Anhaltspunkte, die die Verhaftung Wernery veranlasst haben könnten. Bislang ist auch dem Hamburger Anwalt, Axel Bauer, keine Akteneinsicht zum Stand deutscher Verfahren gewährt worden. Nach Auffassung einiger CCC-Mitglieder kann dies nur daran liegen, dass die vorliegenden Ermittlungsergebnisse derart schwach sind, dass eine anwaltliche Prüfung zur sofortigen Einstellung des Verfahrens führen würde.
Untersuchungsrichter Daniel Fontenaud erklärte, ein Schreiben Wernerys an die französische Philipsniederlassung, das dort als Erpressungsversuch gewertet wurde, sei auch ein Haftgrund. Dem Vernehmen nach ist man mittlerweile auch bei der Philipszentrale in den Niederlanden nicht sehr glücklich über das Vorgehen der französischen Niederlassung. Wie aus gut unterrichteten Kreisen verlautet, existiert ein Gutachten, in dem Wernery als Anstifter verschiedener Unregelmässigkeiten in französischen Computersystemen bezichtigt wird. ähnlich wie im deutschen Verfahren, ist es schwierig, derartige Spekulationen der Ermittlungsbehörden zu entkräften. "Die Vorurteile scheinen in Frankreich den Blick für Tatsachen zu vernebeln", erklärte ein CCC-Mitglied.
Wie aus CCC-Kreisen zu erfahren war, werden derzeit Möglichkeiten einer Kautionslösung geprüft. Da gegen Wernery lediglich ermittelt wird, ist er nach dem Gesetz weder beschuldigt noch angeklagt. Die Untersuchungshaft wird von den französischen Behörden mit "Fluchtgefahr" begründet. Wie Wernerys Anwältin, Eva Sterzing, in Paris gegenüber dem CCC erklärte, liegt die Kaution erfahrungsgemäss zwischen 30.000 und 50.000 Mark.
Frau Sterzing berichtete, dass es Steffen Wernery den Umständen entsprechend gut gehe. Er behielte weiterhin einen klaren Kopf und könne mit der Situation erstaunlich gut umgehen. Wegen der notwendigen Übersetzungen seien die Verhöre sehr langwierig. Dies führe zu einer erheblichen Verzögerung des Verfs. Ein weiteres Verhör ist für den 19. Mai anberaumt. Dabei wird wahrscheinlich auch die Kautionslösung zur Sprache kommen.

"Südwestdeutscher Journalistenverband (SWJV) in der Mediengewerkschaft

Die Delegiertenkonferenz des SWJV wird gebeten sich für den Journalisten Steffen Wernery vom Chaos Computer Club (CCC), Hamburg, einzusetzen, der in Frankreich inhaftiert wurde und angeklagt ist, dem 'französischen Volk' (durch Hackertätigkeit) einen Schaden von vier Milliarden Francs zugefügt zu haben.
Die Delegiertenkonferenz fordert alle Kolleginnen und Kollegen auf, die Kriminalisierung Steffen Wernerys im Ausland anzuprangen, nachdem die deutsche Staatsanwaltschaft (Hamburg) bereits festgestellt hat, dass Wernery nicht selbst an den Hacker-Aktionen beteiligt war, sondern die 'Computer-Kids' deckt, die seinerzeit bis in die NASA-Computer vorgedrungen sind. Wernery deckte erhebliche Sicherheitsmängel auf und bekam vom Hamburger Datenschutzbeauftragten für das Aufdecken des sogenannten NASA-Hack ausdrückliches Lob. Wernerys materielle Existenz ist durch die Untersuchungshaft bedroht. Sein täglicher BTX-Dienst für Computer-Kids kann nicht aktualisiert werden, weil nur er Passwörter und und dergleichen kennt. Der Chaos Computer Club versuchte bereits die deutsche Öffentlichkeit zu erreichen. Die Kolleginnen und Kollegen in Tageszeitungen, Hörfunk und Fernsehen waren in Einzelaktionen nicht zu aktivieren."
Der Aufruf wurde angenommen.

Aus der Gerüchteküche

Angeblich ist Steffen Werneéry seit 20.Mai auf freien Fuß. Diese Meldung wurde am Abend des 20. von RTL gebracht. Bis heute ist es uns nicht gelungen, ihren Wahrheitsgehalt zu überprüfen.

Der Computer-lesbare Personal-ausweis

Der Fälschungsversuch eines Stern-redakteurs.

Hamburg (clinch/stern) - Mit den neuen Plastik-Perso werden wir wohl noch einige Ueberraschungen erleben. Ueber die angebliche Faelschungssicherheit unkte Hamburger Verfassungsschutz-Chef Christian Lochte bereits vor zwei Jahren. In einem STERN- Interview prophezeite er, der neue Personalausweis werde die innere Sicherheit nicht verbessern. Lediglich die Lederwaren-Industrie haette Vorteile: Das Format des Ausweises sei so ungewoehnlich, dass er nicht herkoemmliche Portemonais passt und die Buerger wohl neue Geldboersen kaufen werden.

In der Ausgabe vom 4. Februar 1988 hat der STERN unter dem Titel "Gute Karten fuer Faelscher" die Katze aus dem Sack gelassen. Der Parlamentarische Staatsekretaer im Innenministerium Carl- Dieter Spranger (CSU) konnte einen vom STERN gefaelschten Ausweis nicht als solchen sofort identifizieren. Das der Staatsekretaer ins Schleudern kam, verdankt er einem Laser-Farbkopierer der japanischen Firma Canon, ein Geraet, das seit wenigen Wochen bundesweit in Firmen und Copyshops steht. Die Fachzeitschrift "Criminal-Digest" stellte schon die bange Frage: Kopiert der neue Canon besser, als das BKA erlaubt?

Sternredakteur Thomas Osterkorn machte die Probe aufs Exempel. Von einem Kollegen lieh er sich den neuen Ausweis, schnitt sein eigenes Foto passend zurecht und legte es ueber den Ausweis. Das ganze kopierte er innerhalb von 45 Sekunden mit dem neuen Canon- Geraet. Der Kopierer traf die Farben auf Anhieb nahezu orginalgetreu und reproduzierte sogar die feinen Muster des Papiers so gut, dass nur ein Fachmann bei genauer Untersuchung einen Unterschied erkennen kann. Und - das kopieren ist nichteinmal verboten. Nach Auffassung des Bundesgerichtshofes ist eine Fotokopie keine "Urkunde". Lediglich der spaetere Gebrauch "zur Taeuschung im Rechtsverkehr" ist strafbar. Auch das perfekte Einschweissen in Plastik war kein Problem. Fuer 450.- DM gibt es auf dem Markt einen sogenannten Econo-Laminator, mit dem zahlreiche Firmen ihre Dokumente versiegeln oder Hausausweise herstellen. Die Folien, millimetergenau fuer Personalausweis-Groesse (DIN A 7), gibt es fuer 57 Pfennig im Buerofachhandel.

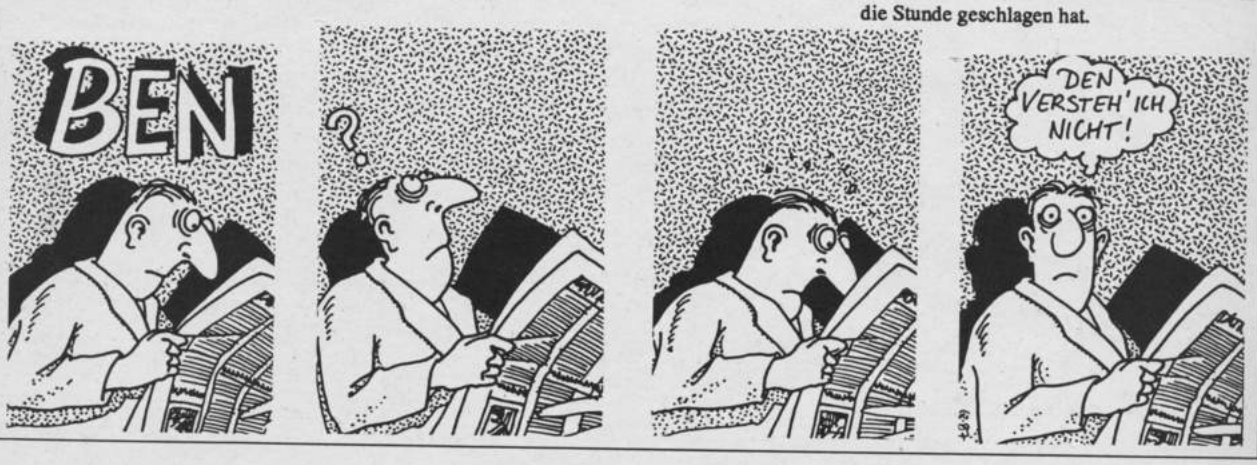
Der "Anwendertest" war denn auch durchaus erfolgreich. Sternredakteur Osterkorn machte sich am 20. Januar 1988 zusammen mit seinem Kollegen Peter Rall auf den Weg nach Bonn - wo sie gegen 18 Uhr Staatssekretaer Spranger trafen.

Osterkorn: "Mein Kollege und ich fragen Spranger nach dem neuen Digital-Farbkopierer: 'Ist damit der faelschungssichere Ausweis nicht doch kinderleicht nachzumachen?'

'Was da bisher angeboten wurde, ist auch fuer einen Laien so klar als Faelschung zu erkennen, dass der Wert des Ausweises sich erst recht erwiesen hat.' Ich gebe Spranger meinen nachgemachten Ausweis und frage, was so eine Plastikkarte den faelschungssicher mache. 'Eine Fotokopie hat beispielsweise ueberhaupt nicht die erkennbare Plastikhuelle, diese Rillen, diese Zusammensetzung, dieses Material", sagt er und zeigt auf meinen Ausweis. Der Staatssekretaer sucht in seinen Akten nach einer Farbkopie eines Ausweises, die ihm seine Referenten besorgt haben, und merkt nicht, dass er bereits eine in der Hand hat.

Auf den Hinweis, mein Ausweis sei eine Kopie, holt Spranger seinen eigenen Personalausweis aus der Tasche, vergleicht beide Exemplare und behauptet, er habe unsere Faelschung gleich erkannt. Doch ausschliessen will er nicht, dass wir auch eine Ausweiskontrolle im Bundesinnenministerium mit diesem Dokument ueberstanden haetten. Und er raeumt ein, er halte es "fuer notwendig, dass die Fachleute des BKA die technische Entwicklung genau und sorgfaeltig beobachten".

Nun ja, was man von den technischen Faehigkeiten des BKA zu halten hat, wissen wir inzwischen auch. Rosige Zeiten fuer Regierung und Polizei. Und wenn der Stern im Zwischentitel der Story feststellt, die neue Eurocheque-Karte sei sicherer als der neue Personalausweis, wissen Insider ohnehin was die Stunde geschlagen hat.



Der Computer als Brutstätte einer neuen Kriminalität

Am 18. Januar 1980 brachte ein New Yorker Fluglotse, aus Ärger über die ein Monat zuvor erfolgte sowjetische Invasion in Afghanistan, vorübergehend ein ankommendes Flugzeug der Aeroflot mit dem sowjetischen Botschafter Anatoly F. Dobrynin an Bord unter seine Kontrolle. Er übergab die Steuerung an seinen Computer, löschte ein Signal, das die Maschine als großes Düsenflugzeug identifizierte, und transferierte die Steuerung dann zurück zum Hauptsteuerpult.

Ohne das Signal erschien der Jet auf den Monitoren der anderen Fluglotsen als kleines Privatflugzeug. Nach einem gefährlichen zwanzigminütigen Flug durch stark frequentierten Luftraum, ohne entsprechende Kontrollen, konnte die Maschine sicher landen. Der Lotse wurde gefeuert, aber nicht strafrechtlich verfolgt.

Letzten Sommer wurde eine Gruppe von jungen Computer-Freaks aus Milwaukee, nach der lokalen Telephonvorwahl auch "Die 414er" genannt, von FBI-Agenten ausgehoben, nachdem sie sich zu mehr als 60 Computer-Datenbanken Zugang verschafft hatten, darunter die des New Yorker Memorial Sloan Kettering Krebsforschungszentrums, des wissenschaftlichen Labors Los Alamos in New Mexico, und einer kalifornischen Bank.

Diese Vorfälle, der eine potentiell tödlich, der andere scheinbar Spielerei, repräsentieren die Auswüchse eines Phänomens, das unter Vollzugsbeamten wachsende Besorgnis ausgelöst hat: Computer-Kriminalität und Mißbrauch.

Experten der Regierung und der Privatindustrie sagen, daß die Vielfalt dieser Verbrechen und die mögliche Schadenshöhe beängstigend sind. Sie erwähnen Urheberrechtsverletzungen, Erpressung, elektronische Bankbetrügereien in der Höhe von vielen Millionen Dollar, Industrie- und Militärspionage, Terrorismus, Sabotage und sogar Mord.

Computer bieten ebenso beunruhigende Möglichkeiten ins Privatleben einzudringen. Wenn es sogar einem jungen Computerwappler gelingt, sich Zugang zu computerisierten Kreditunterlagen, Krankengeschichten, Kfz-Zulassungsdaten, und Bankkonten zu verschaffen, fragen sich die Experten was erst ein Profi anstellen könnte.

Jetzt, da das Land immer stärker computerisiert wird, warnen die Experten, daß zu wenige Anstrengungen unternommen werden, um Gesetze über Computer-Mißbrauch, Sicherheitsmaßnahmen um ihn zu verhindern, neue Versicherungsformen um sich gegen Verluste zu schützen, oder ethische und soziale Fragen die sich durch die obskuren Wunder der elektronischen Informationsverarbeitung stellen, zu erlassen.

Joseph F. Coates, Konsulent für langfristige technologische Entwicklungen, sieht das Problem folgendermaßen: "Die Computerindustrie ist so selbstgefällig, die Käufer und Anwender sind so begeilt von ihrer Ausrüstung, und die Gesetzgeber so eingelullt durch die trügerische Ruhe, die herrscht, während sich die Computer allmählich über das ganze Land verbreiten, daß es eines zweiten Hiroshima bedarf, um das Land aufzurütteln und ihm die enormen Risken, die der derzeitige Computer-Einsatz in sich birgt, vor Augen zu führen."

Die spezifische und wachsende Bedrohung durch Computer-Kriminalität beruht auf diversen Faktoren, darunter:

- **Unsichtbarkeit.** Das Verbrechen kann aus großer Distanz verübt werden, möglicherweise in der Abgeschiedenheit einer Wohnung oder eines Büros. Spuren des Eindringens können in vielen Fällen getilgt werden.
- **Der Microcomputer.** Alexander Stein, Mitarbeiter von Dataquest, einer kalifornischen Konsulentenfirma, sagte, daß es Ende 1983 in den USA 7.9 Millionen Heim- und Personalcomputer sowie mehr als eine Million Bürocomputer gab. Die Zuwachsrate liegt bei 34% pro Jahr, d.h. daß sich die Anzahl der Computer alle 3 Jahre mehr als verdoppelt. Vollzugsbeamten vertreten ausnahmslos die Ansicht, daß die Verbreitung von Personalcomputern einen Zuwachs der Computer-Kriminalität mit sich bringen wird.
- **Computerbildung.** Microcomputer sind bereits in Volksschulen gang und gebe.

Jugendliche besuchen im Sommer Computer-Camps. Teenager können für weniger als 1000 Dollar einen Computer kaufen. Das MIT stellt seinen 4500 Studenten mit Hilfe von IBM und DEC 3000 Computer-Terminals für die Lehre zur Verfügung.

Da nun ein weitaus größerer Teil der Bevökerung lernt mit Computern umzugehen, befürchten Experten einen erheblichen Zuwachs des Computer-Mißbrauchs durch Kriminelle, Unzufriedene und geistig Labile.

- **Netzwerke.** Billige Zusatzgeräte "Modems" genannt, schaffen für Heimcomputer die Möglichkeit mit Computersystemen in aller Welt in Verbindung zu treten. Bereits jetzt werden hunderte Seviceleistungen angeboten, unter anderem: Nachrichten, Börsenkurse, weltweite Flugauskunft, ganze Enzyklopedien, Wettervorhersagen, und sogar Filmkritiken bis ins Jahr 1930 zurück. Der nächste Schritt beinhaltet interaktive, d.h. Zwei-Weg, Dienstleistungen, zum Beispiel: computerisiertes Einkaufen, Fakturieren, Bankgeschäfte und Versand. Diese Innovation nahm kürzlich starken Aufschwung durch ein Joint-Venture von Sears, Roebuck, IBM und CBS.
- **Verbesserte Technologie.** Computer werden immer schneller, billiger und bedienungsfreundlicher und die Speicherkapazität nimmt zu. Daher wird der Computer-Einsatz für komplexere und praxisbezogenere Anwendungen immer lohnender.
- **Intelligentere Computer.** Der Wettlauf zwischen Amerikanern und Japanern bei der Entwicklung von Computern der "5ten Generation", könnte innerhalb weniger Jahre zu Frühformen der AI führen (Anm. des Tippers: wie die Neanderthaler), die ein ungeahntes Potential an Gut und Böse in sich tragen. Marvin Minsky, AI Flachmann des MIT, sagte die Welt der Computer ist an einem Punkt angelangt, von dem ich einst glaubte, es würde Jahrhunderte dauern ihn zu erreichen. In Hinblick auf die Zukunft meint er: "Sie sollten (Robert) Henlein oder (Isaac) Asimov lesen (Science-Fiction Autoren)."

Schätzungen des jährlichen Verlustes durch Computer-Kriminalität reichen von 100 Millionen bis zu mehr als 3

Milliarden Dollar, doch selbst die Experten geben zu, daß die Zahlen aus der Luft gegriffen sind.Anthony Adamski, der FBI-Referent für Computer-Kriminalität erklärte, daß Zahl und Kosten dieser Verbrechen unbekannt seien.

Robert P. Campbell, ein privater Spezialist für Computersicherheit, und bis vor 5 Jahren Leiter der Computer-Sicherheits Abteilung der US-Armee, schätzt daß nur einer von 22.000 Fällen von Computer-Kriminalität strafrechtlich verfolgt wird. Er glaubt, daß eines von hundert Verbrechen entdeckt wird; daß davon maximal 15% gemeldet werden und daß es in einem von 33 gemeldeten Fällen zu einer Verurteilung kommt.

Bundesbeamte sehen die Ursache darin, daß viele Firmen, vor allem Banken, kein Interesse daran haben, die Öffentlichkeit oder iher Aktionäre darüber zu informieren, daß sie Opfer einer solchen Straftat wurden die noch dazu relativ leicht zu begehen war. Außerdem macht es die Registrierung dieser "Bürokriminalität" fast unmöglich festzustellen, ob ein Computer benützt wurde.

Selbst wenn solche Straftaten gemeldet werden, kommt es oft zu keiner Gerichtsver-handlung, weil Staatsanwälte, Richter und Geschworene nicht die Fachkenntnisse haben, um solche Fälle zu bearbeiten.

Trotzdem kommen gelegentlich Computer-Verbrechen in die Schlagzeilen.

Behörden verschiedener Staaten gelang es Fälle aufzudecken, in denen jemand die Bankzahlscheine am Schalter gegen die eigenen Zahlscheine ausgetauscht hat. Wenn nun ein Kunde diese verwendet, um Geld einzuzahlen, so wird dies auf das Konto des Täters gebucht. Wenn die aufgebrachten Kunden mit ihren Kontoauszügen wiederkommen, ist das Geld bereits abgehoben und der Täter entflohen.

1978 rief der Computer-Konsulent Mark Rifkin in der Security Pacific National Bank in Los Angeles an, identifizierte sich als höherer Bank-Angestellter, nannte die richtigen Codes und veranlasste eine Überweisung von 10,2 Millionen Dollar auf ein Schweizer Bankkonto. Er erwarb darum sowjetische Diamanten, wurde aber beim Versuch sie zu verkaufen verhaftet. Er verbüßte weniger als 3 Jahre einer achtjährigen Haftstrafe und arbeitet jetzt als Leiter der Computer-Abteilung einer größeren Organisation.

Richard P. Kusserow, Generalinspektor des Ministeriums für Gesundheit und Allgemeine Dienstleistungen, beendete kürzlich eine Untersuchung über Straftaten im Zusammenhang mit den 650.000 Microcomputern und 16.000 Mainfraimes des Staates, und stellte eine außergewöhnlich hohe Verwundbarkeit fest.

"Der Staat ist der größte Benutzer von Computern in diesem Land. Im Moment erleben wir eine Informationsexplosion ,... die so schnell vor sich geht, daß die Bürokratie noch keine Gelegenheit hatte, zu reagieren."

Die Studie deckte 172 Fälle von Betrug und Mißbrauch in 12 Regierungsstellen in einem Zeitraum von etwas mehr als 4 Jahren auf. Ein Angestellter hat 5 Monate hindurch die Unterschriften auf Sozialbeihilfe-Schecks im Wert von 24.000 Dollar gefälscht, das Geld auf sein Konto umgelenkt und sämtliche Beweise gelöscht. Im Rahmen eines anderen Sozialprogramms gelang es drei Büroangestellten Essensmarken im Wert von 150.000 Dollar zu stehlen, weil ihr Vorgesetzter einen Schlüssel in einem Terminal vergaß.

Kusserow meinte, daß dies nicht einmal die Spitze des Eisbergs sei, da die meisten Verbrechen durch Zufall entdeckt wurden und die Behörden im Grunde genommen keine Verfahren haben um solche Fälle aufzudecken.

David Geneson, ein Rechtsanwalt des Justizministeriums, der sich mit Computer-Kriminalität beschäftigt, stellte fest, daß es kein Bundesgesetz gibt, welches sich speziell mit der Verwendung von Computern bei Straftaten , mit widerrechtlichem Eindringen in Computer, oder dem Lesen privater Files auseinandersetzt.

"Es gibt keine gesetzliche Definition von Computer-Kriminalität. Dies ist ein wesentlich komplexeres Problem, als es den Anschein hat. Falls jemand in einen Computer-Raum der Regierung eindringt und Disketten stiehlt, so ist das Diebstahl von Staatseigentum. Aber wenn jemand auf elektronischem Weg eindringt und die entsprechenden Files kopiert, ist die Rechtslage nicht eindeutig, da nicht wirklich etwas gestohlen wurde."

Adamski sagte, 21 Staaten hätten Gesetze zur Computer-Kriminalität erlassen, die sich allerdings von Staat zu Staat sehr stark unterscheiden und häufig keine Lösung für das Problem der "Hacker" anbieten, die zum Spaß und nicht aus Gewinnsucht in Systeme eindringen.

Ein Gesetz zu erlassen, gibt den Behörden nicht notwendigerweise die Arbeitskräfte oder Kenntnis es zu exekutieren. In Florida wo 1978 das erste diesbezügliche Gesetz erlassen wurde, kamen bislang nur zwei Fälle vor Gericht.

Gegenwärtig liegen dem Kongress eine Reihe von Gesetzesanträgen zur Computer-Kriminalität vor.Einer, der vom Mitglied des Repräsentantenhauses Bill Nelson (Demokrat aus Florida) und vom Senator Paul S. Trible Jr. (Republikaner aus Virginia) eingebracht wurde, fordert eine Strafe von 50.000 Dollar oder eine 5 jährige Haftstrafe für Diebstahl von Computerdaten, oder Mißbrauch von staatlichen oder privaten Computern, die im Wirtschaftsverkehr der Einzelstaaten eingesetzt werden. Eine zweite Vorlage, die vom Demokraten Ron Wyden, Mitglied des Repräsentantenhauses aus Oregon, eingebracht wurde, sieht eine Spezialeinheit vor, die 18 Monate lang, die Ausmaße der Computer-Kriminalität im Kleingewerbe untersuchen soll.

Eine dritte, vom Mitglied des Repräsentantenhauses William J. Hughes (Demokrat aus New Jersey), eingebracht und von einem Unterausschuß befürwortet, sieht vor, daß unrechtmäßiger Zugriff auf Daten, der dem Beklagten mehr als 5.000 Dollar pro Jahr einbringt, zum Staatsverbrechen erklärt wird; die Verwendung oder Veränderung fremder Computerdaten würde als Vergehen eingestuft.

Diese Gesetzesvorlagen nehmen weder auf Personen bezug, die nur interessehalber in Systeme eindringen, noch beschäftigen sie sich mit dem Anzapfen von Computern. Obwohl es gegen das

Gesetz verstößt Telephongespräche abzuhören - selbst das FBI benötigt eine richterliche Verfügung - verbietet kein Gesetz das Abhören eines Datenaustausches zwischen Computern über eine Telephonleitung.

Zusammenfassend kann man feststellen, daß sich die Kongressdebatten darauf konzentrierten, das unbefugte Eindringen von jungen "Hackern" in staatliche oder private Computer, bundesweit zum Verbrechen zu erklären. Aber die meisten Gesetzesvollzugsbeamten und Computer-Sicherheitsfachleute halten Verbrechen von Insidern, die schon Zugang zum System haben, für das wirkliche Problem.

Mary Thornton, 1984, Washington Post

Das FBI veranstaltet Computerkurse zur Verbrechensbekämpfung.

Mit der Invasion von tausenden Kleincomputern in den amerikanischen Haushalten und Büros sind die Exekutivbehörden mit einer neuen Klasse von Kriminalität konfrontiert, deren Waffe der Computer ist. In vorderster Front im Kampfe gegen die Computerkriminalität steht James M. Barko, der die Schulungen für den Bereich Wirtschafts- und Finanzverbrechen an der FBI-Akademie in Quantico leitet. Barko und andere FBI-Computerexperten halten einen Dreiwochenkurs ab, in dem Beamte die Grundbegriffe des Computers und der Programmierung und die typischen Formen des Computerbetrugs kennenlernen.

"Es ist eine andere Welt ", meint Barko über die Substilität und Erfahrung mit dem Bürotäter einen Computer manipulieren. "Wir haben es hier mit einer Art von Priesterschaft zu tun."

Die Kursteinehmer lernen an Hand einer simulirten Bank mit 50 Millonen Dollar Einlagen und 30.000 Konten.Im Laufe des Kurses entdecken die Beamten Fehler von immer größerer Komplexität im Computersystem dieser Bank. Ihre Aufgabe hierbei ist das Auffinden der Fehler ohne dabei den Bankcomputer abzuschiessen. Verdächtige Einlagen oder Abhebungen von Konten von Bankangestellten, deren engere Freunde und Verwandte werden gesucht. Die Kursteilnehmer lernen zu erkennen welche Personen Zugriff auf bestimmte Dateien haben und können so Verdächtige aussieben. Einer der wichtigsten Aspekte ist das Erlernen wie ein Durchsuchungsbefehl für ein Verbrechen geschrieben wird, bei dem das Beweismaterial in erster Linie in elektronischer Form und nicht in physikalischer Form vorliegt und womöglich in einem Computerprogramm versteckt ist.

Beim Versuch ein Verbrechen aufzudecken müssen die Beamten nicht nur auf offentsichtliche Gelttransfers achten sondern ihre Aufmerksamkeit auf subtile Ausgleichmaneuver lenken, die die Bücher wieder ausgewogen erscheinen lassen und so die Tat gut tarnen.

Barko räumt ein, daß seine Absolventen sicher nicht in der Lage sind jetzt Computerfirmen zu eröffnen. Aber sie haben ein Grundwissen und sie wissen wo sie Hilfe erhalten können. In freundlichen Umgebungen, wo das Managment außer Verdacht steht , kann im Allgemeinen Hilfe von der Firma selbst erwartet werden. In weniger freundlichen Situationen kann technische Hilfe von Seiten der Computerhersteller erlangt werden.

Seit 1976 hat das FBI insgesamt mehr als 200 Beamte und ca 88 Untersuchungsrichter geschult und zur Zeit hat der Kurs eine Warteliste von zwei Jahren.

Mary Thornton, 1984, Washington Post

Das Know-How für`s Geschäft

Verbrechen mittels Computer lassen sich in sehr einfache und sehr komplizierte Fälle unterteilen. Am unteren Ende der Skala rangieren jene "Hacker", die in ein System eindringen, um Noten, Kfz-Zulassungsdaten oder Kredit-Zinssätze zu ändern.

Komplexere Vergehen können Gewinn und Sabotage miteinbeziehen. Die vifsten Verbrecher verwenden äußerst schwer erkennbare Methoden, wie:

- **Falltüren** - Lücken in Programmen, absichtlich oder unabsichtlich entstanden, die es einem Programmierer zu einem späteren Zeitpunkt gestatten, unbemerkt in das System einzudringen, um geheime Dateien zu lesen, eigene Programme einzufügen, sowie Daten zu löschen oder hinzuzufügen.
- **Trojanische Pferde** - geheime Anweisungen, die in bestehenden Programmen versteckt sind.
- **Zeit-Bomben** - wie Trojanische Pferde im System versteckt, um dessen Selbstzerstörung zu bewirken.

Ein verärgerter Angestellter könnte eine Zeit-Bombe legen, die nachdem er das Unternehmen verlassen hat, Rechnungen zerstört.

- **Salami-Taktik** - eine spezielle Art des Trojanischen Pferdes, durch das minimale Beträge, meist als Konto-Gebühren kaschiert, von tausenden Bankkunden auf das eigene Konto überwiesen werden.

Mary Thornton, 1984, Washington Post

Es gibt keine absolute Sicherheit

"So etwas wie absolute Sicherheit gibt es nicht. Und falls es sie doch gäbe, könnte man sie nicht bezahlen", meint Robert Courtney, ein Fachmann auf dem Gebiet der Computersicherheit.

Seine Ansichten werden von Susan Headley, 24 und bekehrte "Hackerin", die jetzt eine Sicherheitsfirma in Kalifornien leitet, geteilt: das einzig sichere System, das sie sich vorstellen kann, wäre "in einem Banksafe mit einer 3 Meter dicken Bleitüre, einer internen Stromversorgung und mit integrierter Hard- und Software."

"Es muß von einer einzigen Person bedient werden. Gewähren Sie nur einer weiteren Person Zugriff auf das System, so garantiere ich Ihnen mit 80%iger Sicherheit, daß jemand eindringen kann.", ergänzt sie.

Louis Lushina, von der NASA, sagt: "Wenn man einen Computer und Terminals hat, dann findet sich sicher jemand, der geschickt genug ist, um einzudringen. In einem geheimen System passiert alles in einem hermetisch abgeschlossenen Raum..., zum Beispiel ist die Kommandounterstützung bei einem Raketenstart streng geheim."

Eines der Hauptprobleme bei kommerziellen Systemen ist, gemäß den Experten, daß diese über Telephon erreicht werden können und zudem noch benutzerfreundlich sind. Um ihren Angestellten die Scheu vor Computern zu nehmen, lassen sich viele Firmen auf einfache Identifizierungs- und Kennwortsysteme ein und stellen für diese außerdem Anleitungen zur Verfügung, die von jedem aufgerufen werden können, der Zugriff zum System hat.

Für die meisten kommerziellen Systeme gibt es verschiedene Arten von Sicherheit:

- Physische Sicherheit, dazu gehören verschlossene Türen, eine kontinuierliche Stromversorgung und bewaffnete Wachen.
- Kennwörter. Computerexperten empfehlen, diese möglichst häufig zu wechseln, und mehrere Kennwörter in einer Folge zu verwenden. Allerdings dürfen Kennwörter keine naheliegenden Wörter sein. Benutzer provozieren Probleme geradezu, indem sie Trainingskennwörter, wie z.B. "Test", weiterverwenden.
- Verwendung von Geburts- oder ähnlich personenbezogenen Daten in Verbindung mit Kennwörtern. Forscher untersuchen die Benutzung von Finger- oder Lippenabdrücken bei der Identifizierung.
- Aufteilung von Computersystemen, sodaß Benutzer nur auf benötigte Bereiche des Speichers Zugriff haben.
- Dokumentationsfunktionen, die festhalten wer zu welchem Zweck auf gespeicherte Daten zugegriffen hat.
- Rückruf. Ein Benutzer wählt den Computer an, identifiziert sich mit Namen und Kennwort und wird vom Computer getrennt. Der Computer überprüft dann die Identität und stellt mit einer vorgegebenen Nummer die Verbindung mit dem Benutzer wieder her.
- Verschlüsselungseinrichtungen. Laut Courtney wurden im letzten Jahr Verschlüsselungseinrichtungen im Wert von 20 Millione Dollar an die Wirtschaft verkauft. Der Nachteil dieser Einrichtungen besteht darin, daß ein Krimineller, der sich Zugang zum System verschafft hat, die Daten neu verschlüsseln und dafür Lösegeld verlangen kann.

Robert Campbell, ehemaliger Leiter der Abteilung für Computersicherheit der US-Armee und heute Eigentümer einer Sicherheitsfirma, meint, daß niemand, der Sicherheit ernst nimmt, ein Computersystem mit Telephonanwahl hat. Selbst bei einem strengen Kennwortsystem kann ein ehrfahrener Krimineller die Sicherheitsvorkehrungen problemlos durch Abhören der Telephonleitungen umgehen.

Andererseits haben geschlossene Systeme, speziell bei Behörden, ihre Grenzen, da sie nicht mit anderen Systemen kommuniziern können. "Deshalb ist dem Verteidigungsministerium vieles unmöglich, was in der Industrie gang und gebe ist.", sagte Campbell.

Selbst ein hermetisch abgeschlossenes Geheimsystem, warnt Campbell, schützt nicht vor den eigenen Leuten. Um dieses Problem in den Griff zu bekommen, schlagen die meisten Fachleute wiederholte Sicherheitskontrollen und genau gegliederte Arbeitsabläufe vor, wodurch unbemerkte Eingriffe durch einzelne Angestellte unmöglich werden.

Aber die Sicherheitsexperten arbeiten nach wie vor an Verbesserungen der Sicherheitstechniken. Laut Campbell ermutigt das Verteidigungsministerium die Computerindustrie, die Möglichkeiten, Sicherheitsvorrichtungen in die Hardware einzubauen, zu erforschen. Viele der derzeitigen Sicherheitseinrichtungen hängen von Softwareprogrammen ab, die mißbräuchlich verwendet oder ausgetrickst werden können.

Joseph Coates, Konsulent für langfristige technologische Entwicklungen, meint, daß die neue Richtung für Sicherheitsmaßnahmen die Verschlüsselung sein sollte, also Codierung von Daten, bevor sie über Telephon gesendet werden, und deren Decodierung beim Empfänger.

"Wir haben zwar wenig Möglichkeiten Menschen zu kontrollieren, doch einige zur Kontrolle von Maschinen." Coates schlägt auch einige relativ einfache Änderungen vor. Zum Beispiel könnten Patienteninformationen auf tragbaren Medien wie etwa Magnetkarten gespeichert werden, statt in einem leichter verwundbaren zentralen System.

Außerdem befürwortet Coates eine I.Q Grenze für Bedienungspersonal einzuführen, gemäß der Theorie, daß sehr intelligente Leute mit weitgehendem Zugriff auf das System und genügend Zeit dazu neigen, aus Langeweile herumzuspielen und so Schwächen im Sicherheitssystem zu entdecken.

Mary Thornton, 1984, Washington Post

Aktion Feigenblatt

Der österreichische Datenschutzreport der ARGE DATEN

In einem großangelegten Praxistest haben Mitglieder der ARGE DATEN untersucht, ob das Auskunftsrecht über eigene Daten, das im Datenschutzgesetz verankert ist, von Firmen und Behörden ernst genommen wird. Die Zahl der Gesetzesverletzungen war derartig hoch, daß nicht mehr von einzelnen schwarzen Schafen in der sensiblen Branche der Datenverarbeiter gesprochen werden kann, sondern von einer ganzen Herde.

Wie wird das Datenschutzgesetz umgangen?
Die Tricks der Datenverarbeiter (anhand konkreter Fälle)

Übrig bleibt ein Feigenblatt.
Die Erlebnisse von Österreichern beim Versuch, Auskunft über Ihre Daten zu erhalten.

Wie erfahre ich, wer welche Daten über mich hat?
Datenschutz und Bürgerrecht.

So bekomme ich Auskunft
Die Planung von Datenschutzanfragen

Die großen Österreichischen Datensammler
Ein Blick hinter die Kulissen

Der gläserne Mensch
Für Behörden Wirklichkeit

Was kann mit Daten gemacht werden?
Möglichkeiten moderner informationstechnischer Methoden, mehr aus Daten herauszuholen.

Hintergrundberichte
Volkszählungsgesetz, Wählerdateien, Meldegesetz, Erkennungsdienstgesetz, Behindertengesetz, Statistik,...

Firmen und Behörden in Kurzdarstellungen, die Begriffe des Datenschutzgesetzes, Kontakte und Informationsquellen, Übersicht über wichtige datenschutzrelevante Gesetze.

In vielen Fällen dient das Datenschutzgesetz dazu, die Blößen einer unkontrollierten Datenspeicherung zu verbergen. Es mußte daher in einigen Fällen mittels Gericht oder Datenschutzkommission die Auskunftserteilung erzwungen werden.

Das Buch eignet sich ideal als Nachschlagewerk bei Datenschutzanfragen, als Handbuch für die Planung eigener Datenschutzanfragen und als Hintergrundinformation über den Umfang der Datenvernetzung in Österreich. Es ist für Laien, Praktiker und Fachleute geschrieben.

Subskription und Bestellung:
Der einzigartige Report kann bis 31. August 1988 zum Subskriptionspreis von 160.- Schilling bestellt werden, anschließend ist der Report um 200.- Schilling erhältlich (Umfang rund 220 Seiten). Bestellung an: ARGE DATEN, 1090 Wien, Liechtensteinstr. 94 (PSK Konto 7214.741).
Kostenlose weitere Information!
Der Buchpreis setzt sich aus den reinen Gestehungskosten und einem "Prozeßkostenanteil" zusammen. Als KäuferIn erwirbt man daher das Recht, laufend über die Ergebnisse der Datenschutzprozesse informiert zu werden.

"B.O. und Genossen. Unter Bezugnahme auf Ihre schematisierten Auskunftsbegehren vom 1. Juli 1987 wird Ihnen mitgeteilt, daß nach der geltenden Rechtslage eine spezielle Mitwirkungspflicht des Betroffenen am Verfahren besteht. ... Im übrigen werden Sie auf die Möglichkeit der Verhängung einer Mutwillensstrafe aufmerksam gemacht." (SR SOKOP MA62 Wien)

"Liste der Demonstranten — Verhängung von Strafen, Stand 14.12. 1987" (Beilage F der Bezirkshauptmannschaft Kirchdorf anläßlich einer Verfassungsgerichtshofsbeschwerde im Zuge der Demonstration gegen die Pyhrn-Autobahn)

"Der Behindertenpaß hat den Vor- und Zunamen, das Geburtsdatum und den Wohnort sowie 1. die Höhe der Minderung der Erwerbsfähigkeit und/oder 2. den Bezug von Geld-leistungen wegen Invalidität, Berufsunfähigkeit oder dauernder Erwerbsunfähigkeit und/oder 3. den Bezug eines Hilflosenzuschusses oder einer Hilflosenzulage, einer Pflegezulage, einer Blindenzulage oder einer gleich-artigen Zulage zu enthalten." (Entwurf zum Bundesbehinderten-gesetz)

"..definieren Sie bitte die Zielgruppen, in welchen Ihre Daten möglicherweise zu finden sind." (Rotes Kreuz, Wien)

"Ich kann Ihnen dazu nur mitteilen, daß wir im Zuge der Kandidatur von Herrn SCRINZI zur Bundespräsidentenwahl eine große Anzahl von Werbeadressen erhielten." (H. Nachtmann, Graz)

"Erkennungsdienstlich zu behandeln sind Personen, die im Verdacht stehen, den Tatbestand eines Verbrechens oder eines vorsätzlich begangenen Vergehens gegen Leib und Leben, die Freiheit, fremdes Vermögen, die Sittlichkeit oder den öffentlichen Frieden verwirkt zu haben." (vorläufiger Entwurf den Erkennungdienstgesetzes)

"Der Adressverlag MADRESS ist für uns Dienstleiter und Verwalter der Adressen der Wiener Wählerdatei..." (ÖVP Wien)

Ich bestelle ____ Exemplar(e) der "AKTION FEIGENBLATT" (öS 160.- bis 31.8.1988, dann öS 200.-, es gilt das Datum des Zahlungseinganges auf PSK Konto 7214.741).

Name: _____

Adresse: _____

Unterschrift: _____

☐ Ich habe den Betrag auf das PSK Konto überwiesen
☐ Ich bestelle per Nachnahme
☐ Schicken sie mir bitte eine Rechnung
(Zutreffenden Kaktus bitte ankreuzen)

In ein Briefkuvert stecken und an
ARGE DATEN
1090 Wien
Liechtensteinstr. 94
(PSK Konto 7214.741)
senden.

Networking

The new telematic culture

Künstler verstehen sich als sensible Darsteller und Kritiker der gesellschaftlichen Zustände, als Botschafter der Auswirkungen aktueller Entwicklungen. Diese Charakterisierung trifft zumindest zu, wenn sie mit hochtechnologischen Industrieprodukten experimentieren, wie z.B. mit vernetzten Computern - auf der Suche nach neuen Kommunikations- und Handlungsweisen, nach kreativen und nicht profitorientierten oder militärischen Einsatzmöglichkeiten.

Elektronischer Raum

"The electronic space" ist der phantasieanregende, in alle Bedeutungsrichtungen dehnbare Oberbegriff für ein neues Medium, das eigentlich, würde man den Werkstoff beschreiben, eben nicht Pinsel und Leinwand oder Marmorblock heißen, sondern Silizium, oder floureszierender Phosphor, oder auch Kupfer, Glasfaser, Parabolspiegel oder Kunststofftastatur. Die Organisationsform dieses Mediums, der Zusammenschluß von Computern über Datennetze, scheint zunächst wenig spektakulär zu sein; das entscheidende sind die neuen Inhalte, die übertragen werden: keine Kursnotationen, keine Flugbuchungen, keine Wetterdaten, sondern kreative Ergüsse, die spontan oder wohlgeplant per Text, Bild oder Ton im elektronischen Raum abgestellt werden und nach Bedarf beliebig herauszufischen sind. Die messages überwinden geographische und temporäre Unterschiede durch deren Übermittlung per Lichtgeschwindigkeit und deren Ablegen in elektronischen Briefkästen.

Die verteilte Urheberschaft durchbricht auch institutionelle Grenzen: Die Ideen müssen nicht mehr in Museen oder Galerien auf ein kaufwütiges oder vernissagegeiles Publikum warten; die raumelektronischen Objekte überwinden so endlich autoritäre Strukturen jener, die bestimmen, was Kunst heute ist; eine Schaffung weltweiter autonomer Wirklichkeitsgemeinschaften ist möglich geworden, Gemeinschaften, die durch Bewußtsein, Ideologie und Begehren und nicht durch Territorien und die damit verbundenen Kommunikationseinschränkungen bestimmt sind.

Anlässlich des 50. Gedenkjahres zum Anschluß Österreichs an Hitlerdeutschland läuft an der Hochschule für Angewandte Kunst das Kommunikationsprojekt "2621. Woche". Mehrere Kunsthochschulen in Europa und den USA sind über das EARN-Netz, das dem Austausch wissenschaftlicher Daten dient, miteinander verbunden: McWrite-, McPaint-, und Digitizing-Disketten rotieren rotglühend. Stattfinden soll einerseits eine Darstellung der Umstände, die zum Anschluß führten, und andererseits eine Bestandsaufnahme neonazistischer und faschistischer Strömungen der Gegenwart, einschließlich der subtilen Anwendung der ursprünglich nationalsozialistischen Massenlenkung, die heute Konzerne in ihren Werbe- und Imagestrategien anwenden (z.B. bei der Gestaltung von Firmenlogos).

Andere Projekte bedienen sich des Telefonnetzes, des Amateurfunkdienstes oder kommerzieller Netze wie I.P.Sharp um Slow-Scan- oder Telefax-Bilder zu übertragen.

Networking verspricht somit eine interaktive Kommunikation verschiedener mikrokultureller Systeme, es bietet die Möglichkeit des so notwendigen überregionalen Dialogs. Doch kann dieses Medium die Mensch-zu-Mensch-Kommunikation nicht ersetzen; sie kann höchstenfalls als zusätzliche Form des Informationsaustausches bereichert werden.

Roland Scheidl

Auszug aus einem Diskussionstext zur Vorlesung **"The new telematic culture"** von Roy Ascott, Leiter der Lehrkanzel für Kommunikationstheorie an der Hochschule für Angewandte Kunst:

"(...) Was ich aber zeigen möchte, ist, daß das Zusammentreffen der Telekommunikation und des Computers - für sich alleine schon sehr mächtige Medien - eine paradigmatische Veränderung unserer Kultur darstellt, und ohne übertrieben optimistisch zu sein, hoffe ich, daß damit ein Quantensprung im menschlichen Bewußtsein einhergehen wird. (...) Das Begrenzte, das klar Definierte, das Vereinzelte - unser westliches Erbe - werden durch das Fließende, das Vereinende, das Verschmelzende ersetzt. (...) Im telematischen Bereich kreativ zu arbeiten heißt, nach Unbestimmtheit und Zweideutigkeit suchen und damit zu jonglieren anstatt genau umrissene semantische Ergebnisse anzustreben. (...) Der elektronische Raum des Videooutputs, der von Text und Bild besetzt ist, ist eine neue Art von Raum, der nichts mit dem projizierten Raum des Films oder dem illusionistischen Raum der Fotografie zu tun hat. Er verschmilzt auf einem zweidimensionalen Raum, seine Tiefe ist unendlich.

Technologie-comix

Offener Brief der Fachschaft Informatik an Herrn Prof. Kopetz

Wien, am 25.5.1988

Sehr geehrter Herr Professor,

Innerhalb der Fachrichtung Informatik gibt es nicht allzu viele Dinge, die ganz außer Streit stehen und zu der keine universitätspolitische Opposition existiert. Gewiß zählt dazu die Verbesserung der nationalen und internationalen Reputation der Wiener Informatik, ein Anliegen - so unser Eindruck bisher -, das Sie auch auf Ihre Fahnen geheftet haben. Allerdings sind uns Hinweise zu Ohren gekommen, daß Sie im Zusammenhang mit dem Berufungsverfahren für das Ordinariat »Mensch-Maschine-Kommunikation«[1] von dieser Linie abgekommen sind. Ließ nämlich schon Ihr Verhalten in der Schlußrunde des Berufungsverfahrens den Schluß zu, daß Sie dem weiblichen Anteil an diesem wissenschaftlichen Remis nicht sonderlich zugetan sind[2], so scheint sich die Vermutung zu bestätigen: Es geht denn die Geschichte um, daß Sie anläßlich eines Mittagessens von Professoren mit Frau Prof. Floyd derselben zuerst "durch die Blume" und dann ziemlich direkt zu verstehen gegeben haben, daß Sie Frau Prof. Floyd nicht an der TU haben wollen bzw. ihr ihre Entfaltungsmöglichkeiten an der TU Wien derart "einladend" präsentiert haben, daß ein Wissenschafter der ersten Garnitur[3] gerne darauf verzichten kann.

So sollen Sie etwa mit formaljuridisch spitzer Nadel, wie der Behauptung, gepiesakt haben, daß sich Frau Floyds Tätigkeit an der TU inhaltlich auf den Namen des Ordinariats (»Mensch-Maschine-Kommunikation«) zu beschränken hat. Ein Ansinnen, das an sich schon verwegen ist, ob der gesetzlichen und praktischen Tatsache, daß ein Ordinarius dem anderen nichts vorschreiben kann; ein Ansinnen, das allerdings schlichtweg Heiterkeitswert erhält, ob der Diskrepanz zwischen Ausschreibungstext und Tätigkeit Ihres eigenen Ordinariats[4].

Wir meinen, daß jedem Professor ein gewisser Bereich für "seine" Personalpolitik zusteht: Dazu zählt natürlich die Besetzung der Stellen der eigenen Abteilung; dazu zählt auch die Ausrichtung eines Instituts, wie etwa der »Technischen Informatik«, dessen Aufbau und Zusammensetzung "nach Ihrem Willen" abgelaufen ist; dazu zählen mit anteiligem Maß auch Personalentscheidungen, die die gesamte Informatik betreffen, wobei wohl den Vorstellungen von "Förderern" und "Freunden" einer bestimmten fachlichen Ausrichtung besonderes Gewicht beizumessen ist.

Wir meinen daher auch, daß das genannte Maß überschritten wird, wenn Sie, wie im vorliegenden Fall, die Berufung von Frau Prof. Floyd zu hintertreiben versuchen, weil sie Ihnen persönlich nicht konveniert, obwohl diese die Fachrichtung Informatik an der TU insgesamt zweifelsohne aufwerten wird. Insbesondere unterlaufen Sie derart die Beschlüsse einer Berufungskommission, an deren demokratischer Entscheidungsfindung sie selbst mitgewirkt haben.

Es ist schwierig genug anerkannte Wissenschafter im Bereich der Informatik zu bekommen. Schon deshalb können wir es uns nicht leisten, wegen Ihren persönlichen, inhaltlichen oder gar ideologischen Animositäten auf Frau Floyd zu verzichten.

Im Sinne der Interessen der gesammten Informatik der TU-Wien bitten wir Sie daher, Ihr informelles Kriegsbeil zu begraben und Frau Prof. Floyd davon zu informieren, daß ihr Wirken in Wien keineswegs behindert wird, sondern ausdrücklich erwünscht ist und in gedeihlicher Umgebung von Statten gehen kann.

Die Fachschft Informatik

[1] Im Rahmen des 1986 erstreikten Ausbauplanes, der einen umfangreichen personellen Ausbau der Informatik bis 1990 vorsieht, wurde vom Wissenschaftsministerium 1987 eine Professorenstelle der oben genannten Fachrichtung genehmigt. Die dazu eingesetzte Berufungskommission endete im November 1987 mit einem Berufungsvorschlag, in dem Frau Prof. Christiane Floyd und Herr Prof. Fischer ex aequo als Erstgereihte aufscheinen. (Die endgültige Entscheidung obliegt dem Ministerium, das mit allen vorgeschlagenen Kandidaten verhandeln und abschließen kann. Dabei ist meist üblich, der bzw. dem Erstgereihten den Vorzug zu geben.) Das Ministerium hat inzwischen begonnen, mit Frau Prof. Floyd zu verhandeln; Prof. Fischer ist für einen Lehrstuhl an einer anderen österreichischen Universität im Gespräch.

[2] Mitglieder der Studentenfraktion berichteten gemäß ihrer Auskunftspflicht den Studenten gegenüber, daß es nur einem "Kraftakt" von Prof. Kopetz zu verdanken sei, daß Frau Prof. Floyd nicht als alleinig Erstgereihte aus dem Berufungsverfahren hervorgegangen ist. Hinlänglich bekannt ist, daß Prof. Floyd und Prof. Kopetz schon in ihrer gemeinsamen Zeit als Professoren an der TU Berlin verschiedene Scharmützel ausgetragen haben. Im Sinne der Dynamik von Lehre und Forschung wäre eine Vielfalt (oder zumindest Mehrfalt) der Meinungen äußerst zu begrüßen.

[3] Frau Floyd genießt international einen hervorragenden Ruf, steht neben Wien auch mit Oslo in Verhandlungen, wo Sie ebenfalls als Winner eines Berufungsverfahrens hervorgegangen ist. Darüberhinaus ist wohl damit zu rechnen, daß man Ihr in Berlin ein attraktives Bleibeangebot machen wird. Da Frau Floyd aber Ihrer Heimatstadt Wien in gewisser Weise sentimental verbunden zu sein scheint, wären trotzdem die Chancen gewahrt, Sie hierher zu bekommen, sofern Sie nicht größere Widerstände zu erwarten hätte.

[4] Im Ausschreibungstext für das Ordinariat, auf das Prof. Kopetz berufen wurde, findet man unter anderem »Lehre und Entwicklung allgemeiner Methoden zur Herstellung und Bewertung anwendungsorientierter Softwaresysteme«. Dem läßt sich ohne Kommentar ein kurzer Auszug über den vom betreffenden Institut geleiteten Lehrbetrieb aus dem Vorlesungsverzeichnis (der im konkreten Fall kein schlechtes Abbild der Institutstätigkeiten ist) gegenüberstellen: »Fehlertolerante Systeme - Systemprogrammierung - Fallstudien von Betriebssystemen - M/M-Schnittstellen in Prozessrechnersystemen - Echtzeitsysteme - Regelungstechnik für Informatiker . . .«.

Um Mißverständnissen vorzubeugen: die Fachschaft Informatik begrüßt ausdrücklich Dynamik in Lehre und Forschung.