DM 2,50

Postvertriebsstück
C9927f

Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

Die Datenschleuder Nr. 18

Februar 1987

The Ultimate Message Error

... und weitere Neuigkeiten

aus der Magnetic Media Metropolis

A count: Volkszählung

Ergebnisse des CCC'86: NETWEAVING & Real Hacking

Dokumentation: ComputerViren

Hacker-Meetings

Wichtige Termine 1987

04.03.-11.03.	CEBIT - Hannover Hackertreff Dienstag 16 Uhr am grösstem Poststand, sonst siehe Btx Programm.
18.04.-19.04.	CCC - Hamburg (Eidelstedter Bürgerhaus) II. PC Virenforum. Aufarbeitung der Erkenntnisse, Diskussionen und Workshops (Anmelden!).
18.04.	CCC - Hamburg (Eidelstedter Bürgerhaus) Ordentliche Mitgliederversammlung des CCC e.V.
11.06.-14.06.	C'87 - Köln Hackertreff täglich beim WDR Computerclub, sowie Dienstag 16 Uhr am Poststand.
28.08.-06.09	IFA - Berlin Hackertreff Dienstag 16 Uhr am Poststand, sonst siehe Btx-Programm.
12.09.-13.09.	CCC - Hamburg (Eidelstedter Bürgerhaus) Wochenend-Workshop des CCC, Thema noch offen.
19.10.-23.10.	SYSTEMS - München Hackertreff Dienstag am grösstem Poststand, sonst siehe Btx-Programm der BHP.
28.12.-29.12.	CHAOS COMMUNICATION CONGRESS 1987 - Hamburg Die europäische Hackerparty im Eidelstedter Bürgerhaus.

Weitere Hinweise in den Btx-Programmen:
CCC bundesweit *655321#
CAC Regionalbereich 17 *920163#
BHP Regionalbereich 32 *92049204#

LS23 - hacker.txt

Zukunftswerkstätten 1987

im Rahmen des Programms 'Mensch und Technik - sozialverträgliche Technikgestaltung' des Landes Nordrhein-Westfalen.

Anmeldung bei : Zukunftswerkstätten, Nesenhaus 17, 4030 Ratingen 6
20.- DM als Scheck oder bar beifügen.

27.02. - 01.03.	DIE VERKABELTE FAMILIE - CHANCEN, PERSPEKTIVEN UND GEFAHREN in Kerken
09.03. - 11.03.	ZWISCHEN VIDEO UND COMPUTERNETZEN - POLITISCHES LERNEN MIT NEUER TECHNIK in Soest
20.03	FORUM ZU MENSCHENGEMÄßER INFORMATIONS- UND KOMMUNIKATIONSTECHNIK in KÖln
23.03. - 27.03.	MEDIA-PARK KÖLN - STADTTEIL FÜR MODERNE TECHNOLOGIE, LEBENS-, LERN- UND ARBEITSQUALITÄT in KÖln
30.04. - 03.05.	ZUKUNFT DES LEHRENS UND LERNENS IN EINER VON TECHNIK GEPRÄGTEN WELT in Leichlingen
15.05. - 17.05.	NEUE MEDIEN UND BÜRGERMITWIRKUNG IM KOMMUNALEN BEREICH in Marl
29.05. - 31.05.	WELCHE VORTEILE BRINGT DIE BILDSCHIRMARBEIT DEN FRAUEN? in Bielefeld (NUR für Frauen - für Kinderbetreuung ist gesorgt)
19.06. - 21.06.	DER HARTE UND DER SANFTE WEG? Wege zu einer sozialverträglichen Technik in Berg. Gladbach

1ST Hack

Schon während der Aufbauphase des CCC'86 glückte der erste Hack: Bei Forschungsarbeiten in einem heimischen Großrechner Marke VAX wurde ein Kleinverzeichnis von Computerinstallationen in Moskau, zuzüglich Seriennummern, gefunden. Unter anderem steht dort "1 CBM 8032 und 1 CBM 8250" sowie "1 Tüte mit Bauteilen".
wau

Hacker - Erinnerung und Warnung

(Gruppenleiter, CERN-DD/CS, Sektion EN)

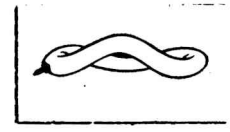
von Giorgio Heimann

"Wir leiden noch immer täglich unter Attacken von Hackern. Zur Zeit können wir an einigen VAXen der CERN ungefähr 20 "Einbruchsversuche" täglich beobachten.
Obwohl wir uns mit Hilfe der CERN-Rechtsabteilung darauf vorbereitet haben, die Schweizer PTT einzuschalten, um herauszufinden, welche Aktionen möglicherweise gegen diese Leute unternommen werden können, bestehen wir jedoch nach wie vor auf dem Prinzip, daß jedes System sich selber zu schützen hat. Dies ist die einzig sinnvolle Lösung, da es einen sehr viel differenzierteren Schutz ergibt; außerdem verlagert diese Strategie die Verantwortung zum Schutz der Betriebsmittel dahin, wo sie hingehört, nämlich zum Eigentümer der Betriebsmittel.
Neben "externem" Hacken haben wir vor einigen Wochen einen Fall einer internen Attacke gehabt. Der Ausgangspunkt des Vorfalls wurde zurückverfolgt und die verantwortliche Person konnte identifiziert werden. Wir beschlossen, diesen Vorfall zu vergessen, da in diesem speziellen Fall keinerlei böser Wille im Spiel gewesen war. Wir mußten aber eine Menge (rarer) Arbeitskraft für die Suche verplempern, so daß unsere Aufmerksamkeit von unseren eigentlichen Aktivitäten und der Überwachung von ernsteren und böswilligeren Attacken abgezogen wurde.
Deshalb seien alle CERN-Benutzer gewarnt, daß wir in Zukunft möglicherweise mit ernsthafter Verfolgung gegen Leute vorgehen, die für "Hack-Attacken" verantwortlich sind."

Aus: "Mini & Micro Computer Newsletter", Dec. '85; Übersetzung: T. Twiddlebit

Datex-P: Auslösung

Entwicklungsfehler



Wenige haben es noch nie erlebt: Auf einmal bricht die Verbindung zusammen, ja, es scheint sogar so häufig vorzukommen, daß schon "Ansagetexte" wie

PATEX-D: Auslösung - Veranlassung durch Durchfall
PATEX-POO: Einlösung - Veranlassung durch Zufall

im GeoNet zu finden sind.

Warum das passiert, liegt häufig daran, daß durch Übertragungsstörungen die zwei an einer Paketübermittlung beteiligten Rechner total aus der Synchronisation laufen, d.h. jede Seite "vermutet" etwas falsches über den Zustand der anderen Seite.
Unglücklicherweise ist nun das X.25 Protokoll, der internationale Standard für viele Strecken im Paketnetz, so konstruiert, daß es nicht selbstsynchronisierend ist. Eine Paketübermittlung mit X.25 ist in einem labilen Gleichgewicht; zu Beginn der Übertragung werden spezielle Initialisierungspakete ausgetauscht, die nur einen eindeutigen Zustand herstellen, wenn die Sende/Empfangspuffer auf beiden Seiten geleert sind.
Resultat: Nach dem Herstellen einer virtuellen Verbindung "vergißt" das Netz manchmal, welche Pakete schon "abgeliefert" sind. Resultat:

DATEX-P: Auslösung - Ablauffehler

Die Gründe dafür sind historischer Natur:
X.25 wurde aus dem IBM SDLC (Synchronous Data Link Control) heraus entwickelt/übernommen. Dabei haben sich in den X.25 Standard Strukturen aus SDLC Tagen eingeschlichen, die inzwischen vollkommen sinnlos sind; andere, für eine Resynchronisierbarkeit notwendige Informationen, werden jedoch nicht übermittelt. Dies ist bei der Weiterentwicklung und Benutzung von X.25 erkannt worden und führte zur Erfindung von immer neuen, speziellen "Steuerpaketen". Kurz: Ein typisches Beispiel für einen im GRUNDE vermurksten Kommittee-Entwurf, der auch durch Einziehen immer neuer Stützbalken nicht richtiger wird.
Folge: Ein Alptraum an Komplexität und Sonderfallbehandlung für jeden Systemprogrammierer, der ein X.25 Protokoll implementieren muß. Zustzlich ist der Wortlaut in den CCITT Dokumenten so vieldeutig, daß Implementationen, die sich an den Text gehalten haben, inkompatibel sind.
Für eine ins einzelne gehende Kritik und - vor allem - einen konstruktiven Vorschlag für ein selbstsynchronisierendes Protokoll (in Pseudo-Pascal), das sehr einfach zu implementieren ist: "Serial Link Protocol Design: A Critique of the X.25 Standard, Level 2" by John G. Fletcher, Lawrence Livermore Lab, erschienen in einem Konferenzbericht der SIGCOMM (ACM) 1984 "Communications Architectures & Protocols"

KS

Strahlengefahr

aus dem Telefon

Wir berichteten in der letzten Ausgabe (ds 17) über ein neues Leistungsmerkmal der Gebührenzähler in Posttelefonen. Inzwischen beschäftigt sich der Bundesbeauftragte für den Datenschutz (BfD) mit diesem Phänomen.
Festgestellt wurde, daß alle mechanischen Gebührenzähler (herkömmlicher Bauart, ca. 1,3 Mio.) einen Fehler im "Begrenzverstärker" aufweisen und dadurch (in Toleranzgrenzen) im Langwellenbereich das Gespräch wie ein Sender ausstrahlen. Dieses Signal wurde mit guten Empfängern beim FTZ noch in 40 cm Entfernung gemessen. Inwieweit metallische Leitungsführungen (z. B. Heizungen) dieses Sendesignal weiterleiten und dadurch die Reichweite verstärken, wurde noch nicht berücksichtigt.
Eine Austauschaktion der betreffenden Gebührenzähler erscheint dem BfD im Verhältnis zum Aufwand nicht angemessen. Vielmehr sollten alle betreffenden Fernsprechteilnehmer über diesen Umstand informiert werden. Desweiteren ist es zu überdenken, die Störstrahlenverordnungen für zukünftige Entwicklungen anzupassen. Bisher entsprechen die "strahlenden" Telefone diesen Vorschriften.
Strahlende Fernsprechteilnehmer erhielten bisher kostenfrei Ersatzgeräte. Derzeit läuft gerade eine Bundestagsanfrage der GRÜNEN zu diesem Thema, über deren Ausgang wir berichten werden.

LS23

STRAHL18.DOC 19870131 2053

DPA hackt

Tief versunken in der Arbeit werkelte am Dienstag, den 9. Dezember 86 die G.ID.-Redaktion (Genethische InformationsDienste; die biologische Datenschleuder) an ihrer nächsten Ausgabe. Plötzlich schrillte das Telefon. Eine Mitarbeiterin der Deutschen Presse- Agentur hatte am Himmel ein Flugzeug entdeckt, welches eine mysteriöse Zahlenkombination in die Wolken über Hamburg schrieb.
Durch kreatives Betrachten konnte die Zahlenreihe 190 119 entziffert werden, wobei sich sofort der Schluß aufdrängte, es könne sich um eine Telefonnummer handeln. Das Telefon wurde angeworfen - und tatsächlich.
DOCH AUF DER ANDEREN SEITE WAR KEINE MENSCHLICHE STIMME - sondern ein merkwürdiger Piepston. Nun sind auch dpa-Journalisten technisch versiert und schlußfolgerten, daß es sich um einen "Computerton" handeln muß. Sofort wurde das hauseigene Texi aktiviert und munter drauflos gehackt. Allerdings ohne Erfolg. Hilfe wurde nun von der angeblich technisch versierten G.ID-Redaktion erbeten. Doch auch diese scheiterte am beschränkten know how.
Um das Gesicht zu wahren, beschloß man, das Problemfeld zu verlagern und "nichttechnische Alternativen" einzuleiten. Ein Anruf beim Flughafen-Tower förderte den Namen des himmelschreibenden Piloten zutage. Dieser, gerade wieder festen Boden unter den Füßen, zeigte sich eher belustigt über die Interpretation des Hauses dpa. Er habe die Telefonnummer 611061 an den Himmel geschrieben, und das wäre die Rufnummer einer Hamburger Taxizentrale. Da hätte dpa wohl einen etwas falschen Standpunkt gehabt und die Zahlen verdreht.
Wer da nun was hinter die Rufnummer 190119 geklemmt hat, ist bis zur Stunde unbekannt. Wie aus gut unterrichteten Kreisen verlautet, wurden erste Recherchen angeleiert. Möglicherweise handelt es sich aber auch nur um ein einfaches Telefax-Gerät. . .
jwi

DPAHAK18.DOC 1987 0131 2000

Stellenanzeige

Wir stellen 1:

- Buchhalter(in)
- Datatypist(in)
- Programmierer(in) für C, Pascal, Basic, 68000 Assembler
- Chefsekretär(in)
- Postbearbeiter(in)
- Archivar(in)

Aber nicht etwa sechs Einzelpersonen, sondern EINE fähige Kraft, die das alles zusammen kann, ohne nach 46.983 Sekunden (bisherige Bestleistung) einen Zusammenbruch zu erleiden. Wir sind ein aufstrebender Verein von Computerchaoten auf der Suche nach den Problemen, für die wir jetzt schon Lösungen haben.

Wir bieten:
———————-
- angenehme Arbeitsatmosphäre in einem typischen Feuchtbiotop
- rasche Aufstiegsmöglichkeiten (ein Teil unseres Archivs lagert auf dem Dachboden) !L- abwechslungsreiche Tätigkeit (jeden Tag ein anderes Datum)
- interessante Sozialleistungen (was wir uns leisten, ist wirklich sozial = gemein)
- angemessene Bezahlung (unserem Konto angemessen)
- eigenverantwortliche Tätigkeit (wir werden Sie schon zur Verantwortung ziehen)
- gleitende Arbeitszeit (Sie haben da zu sein, wenn wir Sie brauchen)
- klare Arbeitstrukturen (Sie erhalten maximal sieben widersprüchliche Auträge)

Wir erwarten:
———————-
- keine Widerrede

Bewerbungen bitte bis gestern an die Re(d)aktion; Lichtbild unnötig, Lebenslauf und Referenzen unwichtig. Wer sich bei uns bewirbt hat eh keine andere Wahl. Gewerkschaftler erwünscht (sofern Mitglied der Gewerkschaft der Sklaven des römischen Reiches).
goblin

Chaos
Communication
Congress

Das PC-Virenforum

Eine Dokumentation in fünf Teilen

von Steffen Wernéry

Teil 1 - Virus Grundlagen, ein geschichtlicher Rückblick
Teil 2 - PC-Virus Grundlagen (basierend auf MS-DOS)
Teil 3 - Der Demovirus für MS-DOS
Teil 4 - Juristische Hinweise
Teil 5 - Thesen und Ansichten

"Ein 'Virus'-Programm, ins Betriebssystem eingepflanzt, gehört zum Gefährlichsten, was ein DV-System bedroht." Zu dieser Aussage kam die in Ingelheim erscheinende Zeitschrift für Kommunikations- und EDV-Sicherheit (KES) im Juli 1985. Vorausgegangen war die erste deutschsprachige Veröffentlichung über Computerviren in der Bayrischen Hackerpost (3/85). Seitdem geistert das Thema durch die Fachpresse und wird von Insidern hinter vorgehaltener Hand diskutiert. Alle bisherigen Veröffentlichungen zu diesem Thema beruhen auf Forschungsergebnissen, die Fred Cohen 1984 an der University of Southern California erarbeitete.

Neuere Erkenntnisse, gerade im Hinblick auf die zunehmende Verbreitung programmkompatibler Personalcomputer (PC's), sind bis heute nicht bekannt geworden.

Mitte 1986 tauchten die ersten PC-Viren in Freeware (Programme zum Tauschen) aus den USA in der BRD auf. In den Folgemonaten gingen in der Redaktion der DATENSCHLEUDER erstmals in Deutschland programmierte Viren für Heim- und Personalcomputer (u.a. MS-DOS) ein. Die ersten Programmierer wandten sich an den Chaos Computer Club (CCC) - wohin sonst?

Obwohl durch entsprechende Veröffentlichungen in der Fachpresse eine Sensibilität für das Gefahrenpotential der Computerviren bei Herstellern von Betriebssystemen, den Systemhäusern und Softwareanbietern vermutet werden sollte, bewiesen unsere Recherchen das Gegenteil. Die Systemhäuser haben oder wollen die Problematik nicht erkennen. Ein Bewußtsein, das zur Information über Risiken verpflichtet, ist dort bisher nicht vorhanden. Vielmehr ist zu erwarten, daß Industrie und Handel das Gefahrenpotential durch Unterlassung von Information fahrlässig fördern.

Die meisten Anwender von Personal-Computern in Industrie, Handel und Handwerk sowie alle privaten Nutzer sind somit dieser Entwicklung schutzlos ausgeliefert.

Der CCC sah sich deshalb veranlaßt, den Chaos Communication Congress '86 (CCC'86) unter den Schwerpunkt "Computer-Viren" zu stellen. Nur eine Öffentliche Diskussion kann eine Sensibilität für diese Entwicklungen fördern und Erkenntnisse über Folgen, Auswirkungen und Schutzmöglichkeiten sammeln und vermitteln.

Ende Dezember wurde in Hamburg das weltweit erste Öffentliche Diskussionsforum über Computerviren für Home- und Personalcomputer abgehalten. Rund 200 Hacker, Studenten und Computerfreaks, davon ca. 20 Programmierer mit Viren-Erfahrungen nahmen an diesem Forum teil.

Diese Dokumentation faßt erstmalig Erkenntnisse und Diskussionen des VirenForums zusammen.

Teil 1

Virus-Grundlagen

Geschichtlicher Rückblick

Allgemeines

Der Begriff "ComputerViren" wurde 1983 von Len Adleman an der University of Southern California im Zusammenhang mit Cohens Experimenten geprägt. Als Computer-Virus wird ein Programm bezeichnet, das die Eigenschaft hat, andere Programme zu infizieren. Jedesmal, wenn ein Virus aktiviert wird (z.B. durch Starten eines verseuchten Programms), kopiert es sich selbst in ein anderes, noch nicht infiziertes Programm. Jedes infizierte Programm ist ein Virenträger und steckt bei Aktivierung wiederum weitere, unverseuchte Programme an. Die Infektion breitet sich, biologischen Viren ähnlich, lawinenartig in einem DV-System oder Netzwerk aus. Das Virus breitet sich auf den legalen Pfaden aus, es benutzt die Autorisierung der infizierten Programme. Anwender mit hohen Zugriffsrechten auf Netzwerken verschleppen das Virus in alle Teile einer DV-Anlage. Dies sind die ersten entscheidenden Eigenschaften von ComputerViren.

Es ist sicher problematisch, für technische Abläufe biologische Begriffe zu verwenden. Die Bezeichnung "Virus" ist ein Sammelbegriff für eine besondere Form organischer Strukturen, die sich nur über eine spezifische Wirtszelle vermehren können. Hierin liegt eine gewisse Ähnlichkeit, denn "ComputerViren" benötigen ebenfalls ein "Wirtsprogramm", das das Virus aufnehmen und verbreiten kann. Obwohl der Vergleich nicht stimmig ist, haben US-Wissenschaftler Begriffe wie "Viren", "Seuchen" und "Infektionen", wegen der Ähnlichkeiten mit biologischen Abläufen, schon vor Jahren geprägt.

Computer-Seuchen

Über sogenannte Seuchen, die mit Hilfe von WirtsProgrammen in DV- Systeme "verschleppt" werden, gibt es Untersuchungen, die zum Teil schon vor 10 Jahren veröffentlicht wurden. Bereits in den 70er Jahren berichteten Anderson und Linde über "Trojanische Pferde", Programme, die gezielt fremde Programme angreifen und dort Funktionsabläufe verändern. Im Gegensatz zu ComputerViren verbreiten sich "Trojanische Pferde" nicht ungezielt, sondern greifen gezielt ein (REM: if you find wordstar then ersetze funktion sichern gegen löschen).

Hinterhältige Bedrohung

Die eigentliche Gefahr der Virenprogramme ist, neben der unkontrollierten Verbreitung, die Einschleusung von manipulierenden Programmabläufen. Das Virus kann als Programm jedwede vostellbare und programmierbare Manipulationsaufgabe mit sich führen und verbreiten. Dadurch wird die Gebrauchsfähigkeit der Computer radikal in Frage gestellt. Das Virus kann ungehindert alle Abläufe verändern, verfälschen, ersetzen oder völlig andere Aufgaben ausführen. Eine perfide Form von Computersabotage, gegen die besonders gängige PersonalComputer ungeschützt sind.

Spärliche Informationen

Bisher lagen nur wenig differenzierte Informationen über erfolgreiche Experimente mit ComputerViren vor. Fred Cohens Versuche auf mittleren und grossen Rechnern wurden wegen deren Gefährlichkeit von den Systemverantwortlichen abgebrochen. Versicherungen und Banken, sowie das Militär halten sich mit ihren Erkenntnissen bedeckt. Aus Industriekreisen war nur gerüchteweise von erkannten Viren die Rede (wer hätte auch den Mut zu sagen: Wir sind verseucht). Professor Dr. Brunnstein (UNI HH) berichtete auf der Pressekonferenz des CCC'86 von einem Virus auf dem Universitätsrechner, der von einem kommerziell genutzten System aus eingegeben wurde. Auch die Technische Universiät Berlin vermutete einen Virenbefall und mußte Anfang '86 einen 14tägigen Ausfall ihrer IBM/4381 (Großrechner mit komfortablem Betriebssystem) hinnehmen, bis der Betrieb mit einer "sauberen" Systemversion wieder aufgenommen werden konnte.

Kein Gefahrenbewußtsein

Rüdiger Dierstein (DFVLR) beschrieb bereits auf der neunten Datenschutzfachtagung am 14. 11. 85 in Köln wesentliche Aspekte des Virus-Phänomens. "Es ist längst bekannt, daß man Programme schreiben kann, die sich selbst in einem Computersystem reproduzieren. Solche Programme können mit bösartigen Eigenschaften versehen sein. Die Reproduktion der Programme samt ihrer unerwünschten Nebenwirkungen kann auf eine Art gestaltet werden, daß andere, beliebige Programme zum Träger werden. Es sind "unauffindbare" Viren möglich, Unterprogramme also, die sich einer systematischen Suche durch Eigenmodifikation (sich selbst verändernder Viruscode) entziehen".

Dierstein mußte sich in der folgenden Diskussion mit "Abwehrreaktionen" auseinandersetzen. Besonders markant fiel die Stellungnahme des IBM-Datenschutzbeauftragten G. Müller aus, der das Virusphänomen als ein theoretisches, in den Softwarelabors längst gelöstes Problem bezeichnete.

So wundert es nicht, daß trotz ausführlicher Informationen ein Gefahrenbewußtsein gegenüber den ComputerViren nicht ausgebildet ist. Gegenmaßnahmen werden vom DATENSCHUTZBERATER (5/86) als "eher dürftig und konventionell" bezeichnet. Referenten von Sicherheitsseminaren meldeten "eine unglaubliche Ignoranz" verantwortlicher Systembetreiber gegenüber der Bedrohung durch ComputerViren. Für den Bereich der Personalcomputer bleibt festzustellen, daß bisher nur der DATENSCHUTZBERATER (10/86) sich dieses Themas angenommen hat. Neue Erkenntnisse waren dort aber ebensowenig zu finden wie in der jüngsten Veröffentlichung der ComputerPersönlich (24/86).

Fahrlässige Informationspolitik

Es bleibt festzustellen, daß ein Bewußtsein über die Bedrohung durch ComputerViren bisher nicht ausgebildet ist. Hinzu kommt, daß die Bereiche Heim- und Personalcomputer unbeleuchtet blieben. Die Industrie hat bis dato jegliche öffentliche Auseinandersetzung mit diesem Thema vermieden. Programmierer von PC-Viren, die sich zwecks Infomationsaustausch mit verschiedenen Firmen in Verbindung setzten, ernteten eher Unverständnis, ("Für welchen Preis wollen Sie Ihr Virus auf den Markt bringen?") aber keine Basis für qualifizierte Gespräche. Es drängt sich der Verdacht auf, daß bisher keine Abwehrstrategien entwickelt wurden und deshalb dieses Thema absichtlich totgeschwiegen wird. Totschweigen ist bekanntlich kein Abwehrmitttel, eher wird der unkontrollierten Verbreitung dadurch Vorschub geleistet.
Soweit der geschichtliche Rückblick.

Teil 2

Das PC-Virus

Grundlagen, basierend auf Erfahrungen

mit dem Betriebssystem MS-DOS

Im folgenden sollen, zur Vermittlung der Grundlagen, einige VirusFormen erläutert und auf deren Verbreitungsverhalten eingegangen werden. Darüber hinaus werden Hinweise über mögliche Manipulationsaufgaben und den Schutz gegen ComputerViren gegeben. Die Informationen beziehen sich auf Erfahrungen mit dem Betriebssystem MS-DOS, die auch für ähnliche Betriebssysteme gelten.

Funktionsweise einiger ComputerViren

ComputerViren können sich auf unterschiedliche Arten in Programmbeständen verbreiten. Dabei können die betroffenen Programme in ihrer ursprünglichen Funktion gestört werden. Zur Differenzierung erläutern wir, auf der Basis der Erkenntnisse, die Ralf Burger Mitte 1986 dokumentierte, die wesentlichen Unterschiede zwischen
— überschreibenden
— nichtüberschreibenden und
— speicheresidenten
Viren.

Ein ComputerVirus besteht aus mehreren Programmteilen. Um bereits infizierte Programme zu erkennen, versieht das Virus diese Programme mit einem ErkennungsMerkmal (M). Der Programmteil mit der Verbreitungsaufgabe wird als Viruskern (VIR) bezeichnet. Zusätzlich kann über das Virus eine Manipulationsaufgabe (MAN) verbreitet werden. Vor der Ausführung der ursprünglichen Programmaufgabe muss das betroffene Programm eventuell durch eine Verschieberoutine (VER) wiederhergestellt werden.

M = ErkennungsMerkmal
VIR = Verbreitungsaufgabe (Virulenz)
MAN = Manipulationsaufgabe
VER = Verschieberoutine

Funktionsweise überschreibender Viren

Überschreibende Viren beeinträchtigen oft die Funktionsabläufe der infizierten Programme. Das Virus überschreibt einen Teil des vom betroffenen Programm belegtem Speicherplatzes. Dabei wird das Programm zer- oder gestört, wobei das Virus nicht durch Erhöhung des Speicherplatzes auffällt.
Um ein ComputerVirus einzuschleusen, wird ein sogenanntes Trägerprogramm mit dem Virus infiziert. Das Trägerprogramm weist bei der Ausführung keinen Fehler auf, da das Virus entsprechend sorgfältig eingepaßt wurde. Wird das Trägerprogramm als nützliches Hilfsprogramm getarnt, kann die Verbreitung z.B. durch die Neugier des unbedarften Anwenders gestartet werden.

```
! M ! VIR ! MAN !  1. Programm  !
```

Wird das 1. Programm aktiviert, findet das Virus beim Suchen im Inhaltsverzeichnis des Datenspeichers (vorzugsweise Festplatten) ein 2. Programm. Wenn dieses bereits das ErkennungsMerkmal aufweist, wird weitergesucht.

```
! 2. Programm                    !
```

Der Viruskern kopiert das vollständige Virus in das 2. Programm hinein und überschreibt dabei den für das Virus benötigten Speicherplatz am Programmanfang. Das geänderte Programm wird abgespeichert und die MANipulationsaufgabe des Virus wird ausgeführt. Erst danach wird das 1. Programm ausgeführt.

```
! M ! VIR ! MAN !  . . .  Rest des 2. Programms  !
```

Beim Starten des 2. Programmes findet zuerst die Übertragung in das 3. Anwenderprogramm statt. Das 2. Anwenderprogramm arbeitet eventuell fehlerhaft, da Programmteile durch das Virus überschrieben wurden.

```
! M ! VIR ! MAN !  . . .  Rest des 3. Programms  !
```

Dieser Verbreitungsvorgang wiederholt sich bis zur totalen Durchseuchung des Systems. Bei diesem Virus-Typ kann das Virus als das letzte funktionsfähige Programm übrigbleiben.
Bei geschickter Programmierung des Virus bleiben auch bei überschreibenden Viren einige Programme funktionsfähig. In einem relativ großem Buffer (von Programmen reservierter Speicherplatz) lassen sich Viren gut verstecken. SideKick läuft in wesentlichen Funktionen auch mit einem Virus dieser Form. Es stellt dadurch ein Risiko beim Programmtausch dar, denn Viren dieser Form können darin unbemerkt verbreitet werden.

Funktionsweise nicht überschreibender Viren

Nicht überschreibende Viren vergrößern den Speicherplatz des infizierten Programmes. Die betroffenen Programme bleiben funktionsfähig.
Zum Zweck der Einschleusung ist ein Programm bewußt mit einem Virus infiziert worden. Es tritt bei der Ausführung kein Fehler auf.

```
! M ! VIR ! MAN ! VER !  1. Programm  !
```

Der Viruskern findet beim Suchen ein 2. Programm. Wenn dieses Programm das ErkennungsMerkmal aufweist, wird weitergesucht.

```
!  2. Programm  (Teil 1 und 2)  !
```

Um den Speicherplatz am Programmanfang neu zu belegen, kopiert das Virus einen Teil des 2. Programmes, welcher der Länge des Virus entspricht, an das Ende des Programmes.

```
! 1. Teil        ! 2. Prgrm T. 2  !
! 1. Teil        ! 2. Prgrm T. 2  ! 1. Teil        !
```

Der Anfang des 2. Programmes ist nun zweimal vorhanden. Jetzt legt das Virus hinter dem ans Ende kopierten Programmanfang die Verschieberoutine (VER) ab.

```
! 1. Teil        ! 2. Prgrm T. 2  ! 1. Teil        ! VER !
```

Das Virus kopiert sich nun selbst an den Beginn der Datei und überschreibt dabei den 1. Teil des Programmes. Es speichert die geänderte Version ab. Anschließend wird die MANipulationsaufgabe, und danach das 1. Programm ausgeführt.

```
! M ! VIR ! MAN !  2. Prgrm T. 2  ! 1. Teil        ! VER !
```

Beim Starten des 2. Anwenderprogrammes findet zunächst die Übertragung des Virus in das 3. Anwenderprogramm statt. Danach wird die MANipulationsaufgabe ausgeführt. Nun folgt ein Sprung zur Verschieberoutine. Diese Routine kopiert im Arbeitsspeicher den 1. Teil des Programmes wieder an den Dateianfang. Dadurch wird das Virus im Arbeitsspeicher Überschrieben.

```
! 1. Teil        ! 2. Prgrm T. 2  ! 1. Teil        ! VER !
```

Im Arbeitsspeicher steht jetzt wieder die Orginalversion des 2. Programmes. Die Verschieberoutine beendet ihre Aufgabe mit einem Sprung zur Startadresse am Dateianfang. Das 2. Programm wird nun fehlerfrei abgearbeitet; das 3. Programm ist infiziert worden.
Vor dem Starten des 2. Programmes:

```
! 3. Programm                !
```

Nach dem Starten des 2. Programmes:

```
! M ! VIR ! MAN !  3. Prgrm T. 2  ! 1. Teil        ! VER !
```

Besondere Formen von ComputerViren

Funktionsweise speicherresidenter Viren.
Speicheresidente Viren sind eine Sonderform von ComputerViren. Der Unterschied liegt in der Form, in der sie tätig werden. In der Verbreitung gilt für sie praktisch das gleiche wie für alle anderen Virentypen. Beim Starten eines infizierten Programmes werden vor Programmausführung die Verbreitungsaufgaben, die Manipulationsaufgabe und die Verschieberoutine des Virus in ungenutzte Bereiche des Arbeitsspeichers kopiert. Dort hinterlegt, wird das Virus seine Aufgaben wesentlich flexibler erfüllen.
Im Arbeitsspeicher hinterlegte Programme (also auch Viren) können durch einen Interrupt (Meldung des Betriebssystems) aktiviert werden. Dadurch kommen diese Viren wesentlich häufiger zur Ausführung als solche, die nur beim Starten infizierter Programme ausgeführt werden. So genügt es schon eine Diskette in ein derart verseuchtes System einzulegen. Wird diese Diskette vom Betriebssystem erkannt, startet das Virus gleich einen Angriff und kopiert sich in ein Programm auf dem Datenträger. Der Ausbreitungsdrang speicheresidenter Viren gilt als äußerst aggressiv. Alle auf dem betroffenem DV-System benutzten Disketten können die "Seuche" verschleppen.

Mutierende Viren

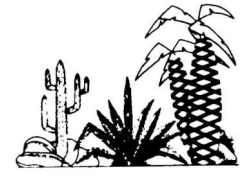
Mutierende Viren ändern bei jedem Verbreitungsvorgang ihre Form. Dieses kann eine Veränderung der Manipulationsaufgabe sein (jedes Anwenderprogramm macht andere Fehler) oder auch nur ein Vertauschen der Programmteile eines Virus innerhalb des Speicherplatzes. Mutierende Viren könnten sich z.B. selbst in Baukastentechnik bei jeder Infektion neu zusammensetzen. Dadurch wird die Suche nach einem erkannten Virus erheblich erschwert.

Ängstliche Viren

Eine besondere Abart sind Viren, die bei einer Aktivierung zwei (oder mehrere) Infektionen in unverseuchten Programmen durchführen und sich anschließend selbst aus dem gestarteten Programm entfernen. Wird dem Anwender bewußt, daß das eben gestartete Programm befallen ist, ist die Seuche schon weitergezogen.

Die MANipulationsaufgabe

Die Verbreitungsfähigkeit der Viren ermöglicht das unkontrollierte Einschleusen von Manipulationsaufgaben. Diese Aufgaben können frei nach der Leistungsfähigkeit des ausgewählten Betriebssystems gestaltet werden.



Der Phantasie keine Grenze gesetzt. . .

Der Phantasie eines VirenProgrammierers sind kaum Grenzen gesetzt. Da davon auszugehen ist, daß Viren, die ihre Manipulationsaufgabe gleich nach dem ersten Infektionsvorgang beginnen, relativ schnell auffallen, geben viele Programmierer den Viren eine Schlafroutine mit auf die Reise. So kann das Virus eine hohe Verbreitung finden, bevor die Manipulation in verseuchten Systemen auftritt und der Virusbefall erkannt wird. Um den Ursprung einer Verseuchung zu verdecken, könnten z.B. die ersten tausend infizierten Programme zusätzlich einen Regenerationsaufrag erhalten. Noch vor Inkrafttreten des Manipulationauftrages löschen sich diese Viren aus ihren Wirtsprogrammen heraus. Eine Analyse des Infektionsweges (wer hat wen verseucht) ist dadurch fast unmöglich.

Ausschlaggebend ist der Zweck

Für das Opfer ist es von wesentlicher Bedeutung festzustellen, welcher Zweck mit einem Virenangriff verfolgt wird. Es kann hilfreich sein, festzustellen, ob bestimmte Daten zum Vor- oder Nachteil Dritter gezielt verändert wurden, um den Schaden, die Folgen und den möglichen Täterkreis einzugrenzen. Handelt es sich "nur" um eine ungezielte Verseuchung, so kann womöglich eine hinterlistige Sabotage zum Vorteil Dritter ausgeschlossen werden.
Auf dem CCC'86 berichteten Teilnehmer über verschiedene Manipulationsaufgaben von Viren. So gibt es Viren, die Daten aus unzugänglichen Speicherbereichen in für den Anwender zugängliche kopieren. Es wurde von einem Virus berichtet, der über jedes infizierte Programm eine "LogDatei" anlegt, in der notiert wird, wer wann mit welchem Kennwort dieses Programm benutzt hat. Weiter wurde von Viren berichtet, die Programme und/oder Daten zerstören, bzw. verfälschen. Sie finden vorwiegend in Freeware und Raubkopien Verbreitung.
Der Schaden und/oder Nutzen eines Virus hängt vom Entwickler bzw. den Verbreitern eines Virus ab. Wohl die Hauptursache für "Rache" sind schlechte soziale Bedingungen für Programmierer. Daneben fördern Neid, Mißgunst und Ohnmacht die Bereitschaft zum böswilligen Vireneinsatz. Die Hauptgefahr sieht Rüdiger Dierstein (DFVLR) im vorsätzlichem Handeln. Die Wahrscheinlichkeit durch Spieltrieb ("Mal sehen was passiert") ein System zu infizieren, stellt ebenso ein Risiko dar. Statistisch unwahrscheinlich ist für Dierstein auch die unabsichtliche Generierung von Computerviren auf dem eigenen DV-System, zum Beispiel durch eine Ansammlung zufälliger Speicherreste.

Auch positive Ansätze

Inwieweit ComputerViren auch zu positiven Aufgaben eingesetzt werden können, hängt von der Isolation des betroffenen DV-Systems ab. Zwar lassen sich Viren auch mit "guten" Eigenschaften versehen, wie z.B. eine Routine, die Daten komprimiert und dadurch den Speicherbedarf senkt. Jedoch kann auch ein solch "guter" Virus bei unkontrollierter Verbreitung für Ärger sorgen.
Vorteilhaft ist die Verbreitungseigenschaft nur, wenn nachträglich in alle Programme zusätzliche Funktionen eingebaut werden sollen. Dieses könnte z.B. ein Virus sein, der die Programme um eine Kennwortabfrage erweitert. Möglich ist auch ein Virus zur Mitarbeiterkontrolle. Einmal ausgesetzt, liefert dieses Virus fortan genaue Nutzungsdaten der Mitarbeiter. Damit lassen sich Unregelmäßigkeiten in der Anwendung erkennen ("ZimmermannVirus").

Viren als Diebstahlsschutz

Rechtlich womöglich zulässig, aber dennoch fragwürdig, sind Viren als Diebstahlsschutz. Softwareanbieter wären in der Lage, auf Messen ihre Programme mit Viren zu versehen, um dadurch nach einer Entwendung der Software den Verbreitungsweg von Raubkopien zu verfolgen.

Vireneigenschaft als Architekturprinzip?

Viren mit kontrollierbaren Verbreitungswegen können positiv genutzt werden. Inwieweit die virulente Eigenschaft neue Architekturen in der Gestaltung von Betriebssystemen und Programmen ermöglicht, ist noch unbekannt.

Erkannte Verbreitungswege von ComputerViren

Risikogruppe Personalcomputer

Derzeit sind alle Personalcomputer für einen Virenbefall prädestiniert. Zum einen verwenden viele Anwender Computer mit weit verbreiteten Betriebssystemen (z.B. MS-DOS), zum anderen tauschen viele der Anwender ihre Programme untereinander und leisten der "Verseuchung" dadurch Vorschub.

Verschleppte Seuche

"Häufiger Diskettentausch mit wechselnden Partnern birgt ein hohes Infektionsrisiko". Die bei Personalcomputern am häufigsten bekanntgewordene Verbreitungsform von Viren findet auf Disketten statt. Congressteilnehmer bestätigten, daß Freeware (Programme zum Tauschen) bisher häufig als Seuchenträger mißbraucht wurden. Dies wirft leider ein schlechtes Licht auf eine an sich positive Form der Softwareverbreitung.

Vorsätzliche Sabotage

Herkömmliche Personalcomputer bieten oft keinen Schutz gegen Fremdbenutzung. An den Stellen, wo technische Hilfsmittel (Schlösser, Chipcard) den Zugriff begrenzen, könnten sich Saboteure die menschliche Unzulänglichkeit zunutze machen. Wird ein Virus in einem Spielprogramm versteckt, reicht es, die Diskette in die Nähe der DV-Anlage zu bringen. Irgendein Neugieriger wird das Spiel leichtsinnigerweise ausprobieren.
Viren können über jede zugängliche Eingabeschnittstelle in eine DV- Anlage gelangen. Dieses könnte die Konsole eines unbeaufsichtigten Terminals sein oder eine Fernzugriffsmöglichkeit wie die Fernwartung. Es ist auch denkbar, ComputerViren versteckt in eine zum Abruf angebotene Telesoftware, etwa aus dem Bildschirmtextsystem, auf den eigenen Rechner zu laden.

Viren sind bei ihrer Ausbreitung nicht auf Schwachstellen oder verdeckte Kanäle angewiesen. Ist ein Virus erst einmal in ein DV-System gelangt, breitet es sich auf den legalen Pfaden der Benutzer aus. Wird das Virus als wichtige Utility (Hilfsprogramm) gekennzeichnet, so steigt womöglich das Bedürfnis der Anwender dieses Programm zu testen. Auf diesem Wege wird das Virus in alle Zugangsbereiche des jeweiligen Anwenders und/oder des Programmes verschleppt.

Schutz vor Viren

"Viren sind dann gut, wenn der Entwickler des Virus das Serum nicht entwickeln kann" so ein Teilnehmer des CCC'86.

Isolierte Systeme

Isolierte Systeme bieten Saboteuren wenig Angriffsmöglichkeiten. Ein isolierter Personalcomputer kommt jedoch selten vor. So werden beim Militär die Wechselplatten (u.a. Wang 20MB) aus der Zentraleinheit herausgenommen und im Tresor verschlossen. Aber auch dort besteht die Gefahr, daß dem Anwender ein infiziertes Programm untergeschoben wird.

Keine "fremden" Programme

Einfach, aber unpraktikabel ist die Methode keinerlei Fremdsoftware auf dem Rechner zu starten, geschweige denn einzusetzen. Beim Kauf orginalversiegelter Programme ist eine Gefährdung im Prinzip weitgehend ausgeschlossen. Kommerzielle Anbieter können es sich aus haftungstechnischen Gründen nicht leisten, Software mit virulenten Eigenschaften zu vertreiben.

Gefahr des Verschleppens

Es ist möglich, daß ein Virus von einem infiziertem System durch den Servicehändler verschleppt wird. Ebenso ist unklar, inwieweit anwenderspezifische Programmpakete nicht durch Fahrlässigkeit des Händlers oder Herstellers verseucht sein könnten.
Vorsicht ist geboten bei Programmen, die z.B. aus Mailboxsystemen geholt oder von "Freunden" kopiert wurden. "Einem Programm - und damit letztlich dem ganzen DV-System - kann man nur genau soviel und genau so wenig Vertrauen schenken, wie dem, der es geschrieben hat". Zu dieser Erkenntnis kam der DATENSCHUTZBERATER (10/85).

Vorsätzliche Manipulation

Da von den Herstellern kaum technische Zugriffsbeschränkungen angeboten werden und diese auch nur selten von den Anwendern genutzt werden, stellt die Überwachung der befugten Rechnernutzung ein bis heute nicht gelöstes Problem dar. Neben Zugriffsmöglichkeiten durch Dritte sollte der Schutz vor böswilligen Mitarbeitern nicht vergessen werden. Sicherheitssensible Leiter von Rechenzentren lassen ihre Programmierer bei Ausspruch der Kündigung nicht mehr an die Rechner und ändern alle relevanten Fernzugriffsmöglichkeiten.

Schwer erkennbare Verseuchung

Um ein Virus zu erkennen, muß festgestellt werden, ob das mutmaßliche Virus andere Programme infiziert. So einfach diese Regel ist, so schwer ist es, sie zu befolgen. Tatsache ist, daß man Programme schreiben kann, von denen nicht feststellbar ist, ob sie sich wie ein Virus verhalten oder nicht.
Bei geschickter Programmierung fallen Viren auch nicht durch langsamere Lade- oder Laufzeiten der Programme auf. Viren mit hoher Rechenzeit könnten lokalisiert werden. Klar sollte jedoch sein, daß bei aller Sucherei ein einziges überlebendes Virus in den Datenbeständen genügt, um die Infektion erneut zu starten.
Vergleichsprozeduren zwischen gesicherten Programmen und den auf aktuellen Festplatten gespeicherten Programmbeständen ermöglichen das Erkennen von Unterschieden wie Länge und Inhalt. Das die "Seuche" auslösende Programm kann aber schon vor Monaten in die gesicherten Datenbestände übernommen worden sein. Die Verbreitung kann dadurch jederzeit wieder gestartet werden.
An dieser Stelle sollte erwähnt werden, daß Viren fähig sind, alle Schreibschutzattribute (Ausnahme Hardwareschreibschutz an der Diskette), Datums- und Namenseinträge zu ignorieren, beziehungsweise wieder herzustellen. Ein infiziertes Programm muß auch nicht unbedingt seine geänderte Länge anzeigen; ein für den C64 entwickelter Virus täuscht die ursprüngliche Länge im Verzeichnis geschickt vor.
Eine Hilfe für Anwender ist ein hardwaremäßiger zuschaltbarer Schreibschutz für Festplatten. Damit könnte geprüft werden, ob Programme, die nur eine Leseberechtigung haben, unberechtigterweise auf die Festplatte schreiben wollen. Dies ist eine Möglichkeit, bei der Installation neuer Software das Verhalten der Programme zu überprüfen. Gegen Viren, die sich erst mit Verzögerung verbreiten, hilft diese arbeitsintensive Methode jedoch nur bedingt.

Hilfe durch "Kontrolldatei"

Eine begrenzte Möglichkeit sahen Congressteilnehmer darin, über ihre Datenbestände eine Prüfsumme anzulegen. Bei einem Virenbefall würden dann die infizierten Programme erkannt werden. Jedoch muß bei dieser Methode eine vollständige Isolation der Prüfprogramme gewährleistet sein. Ein Virus könnte sonst Prüfsumme oder Prüfprogramm gezielt angreifen.
In diesem Zusammenhang erhielten wir von Ralf Burger Hinweise über ein "Schutzprogramm" (MS-DOS), welches unter anderem auf der Basis von Kontrolldateien arbeitet. Sobald dieses Programm seine Funktionssicherheit unter Beweis gestellt hat, werden wir darüber berichten.

Was tun Wenn?

Ohne einen umfassenden vorbeugenden Schutz vor ComputerViren ist es bei einem Virenbefall um die entsprechende Datenverarbeitungsanlage schlecht bestellt. In jedem Fall sollte keine Software mehr verbreitet werden. Ebenso müssen alle Tauschpartner umgehend informiert werden. Weiterhin sollten alle Datenbestände von den Programmen getrennt gesichert werden. Die "verseuchten" Programmbestände müssen isoliert werden und dürfen keinesfalls mehr mit dem System genutzt werden.

Unter Umständen läßt sich aus den "verseuchten" Programmbeständen das Virus und deren Manipulationsaufgabe isolieren. Gelingt dies, so besteht Hoffnung, den ordnungsgemäßen Stand der manipulierten Daten wiederherzustellen. Andernfalls sind die vermutlich manipulierten Datenbestände Grundlage für den weiteren Betrieb der DV-Anlage.
Zur Verarbeitung der Daten wird eine vollständig neue Programmoberfläche benötigt. Deshalb sollten alle Programme erneut von den Herstellern angefordert werden.
Anzumerken sei an dieser Stelle, daß der Geschädigte den Schaden eines Virenbefalls selber tragen muß, wenn er den "Saboteur" nicht überführen kann. Dies ist auch Voraussetzung für die Inanspruchnahme üblicher "Mißbrauchs-Versicherungen". Ein lückenloser Schuldnachweis ist jedoch bei ComputerViren kaum möglich.

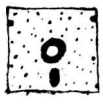
Mehr Forschung und Information

KES (4/85) ruft zur Intensivierung der Forschung auf diesem Gebiet auf. Forschungsergebnisse sollen zukünftige Entwicklungen von Abwehrmaßnahmen ermöglichen. Ziel ist es: Die Risikoschwelle (schnellere Entdeckung) für den Eindringling zu erhöhen. Weiterhin wurde dort die Erstellung eines Sofort-Maßnahmen-Katalogs gefordert. Das spiegelte sich auch in den Beiträgen der Congressteilnehmer wieder. Konsens des Congresses ist, daß nur durch Aufklärung und Information ein Bewußtsein für diese Entwicklung gefördert werden kann und muß. Der CCC wird dieses Thema auf einem II. PC-VirenForum im April weiterbehandeln.

Teil 3

Das Demoprogramm VIRDEM.COM (MS-DOS)

Auf dem CCC'86 wurde im Rahmen des VirenForums ein DemoVirus vorgestellt. VIRDEM.COM wurde von Ralf Burger entwickelt, um die Möglichkeit eines gefahrlosen Arbeitens mit Viren zu bieten. Das Demoprogramm mit Hinweistexten ist von der Redaktion zu beziehen (MS- DOS 360KB Disk oder über Btx als Telesoftware). Das Programm verdeutlicht, wie hilflos ein Anwender gegenüber Computerviren ist, wenn er nicht entsprechende Sicherheitsvorkehrungen trifft.
Das Programm VIRDEM.COM ist ein relativ harmloses Virus, das Programme nicht zerstört und nur auf Diskettenlaufwerk A zugreift. Das Virus erweitert seine Wirtsprogramme um eine zusätzliche Funktion. Außerdem mutiert das Virus seine Funktion bis zur 9. Generation.



Die Funktion des Virus ist ein Ratespiel. Beim Start eines infizierten Programmes meldet sich das Virus "VIRDEM Ver.: 1.0 (Generation ?) aktiv" und fragt eine Zahl ab. Je nach Virengeneration liegt diese Zahl zwischen null und neun. Bei einer Fehleingabe wird das Wirtsprogramm nicht ausgeführt.
VIRDEM.COM wurde entwickelt, um allen MS-DOS Anwendern die Möglichkeit zu bieten, sich mit Computerviren zu beschäftigen, ohne den Gefahren eines unkontrollierten Virenbefalls ausgesetzt zu sein. Sofern die Handhabungshinweise beachtet werden, besteht keine Gefahr einer unbeabsichtigten Verbreitung.
Die Redaktion geht davon aus, daß nur mit sehr hohem Aufwand weitere bösartige Manipulationen in den DemoVirus eingebaut werden können. Achten Sie trotzdem darauf, aus wessen Händen Sie das DemoVirus erhalten. Die Redaktion versendet auf Wunsch die Orginalvirendiskette versiegelt.

Teil 4

Juristische Hinweise zum Umgang mit ComputerViren

Die Thematik juristischer Konsequenzen beim Umgang mit ComputerViren wurde im Rahmen des VirenForums nicht detailliert behandelt. Die Diskussion auf der CLINCH-Mailbox zeigt allerdings eine unerwartete Resonanz zu diesem Thema. Im folgenden einige Auszüge.

Experimente mit ComputerViren

Experimente mit Computerviren bedürfen einer gewissen Sorgfaltspflicht. Gewissenhafte Programmierer sollten sich nicht dem Vorwurf unlauterer Absichten fahrlässig aussetzen.
"Man sollte auf jeden Fall darauf achten, daß man keine Programme weitergibt, die ohne weiteres Zutun Dritter die wesentlichen Eigenschaften eines Virus entwickeln. Desweiteren sollte man Virus- Programme sicher aufbewahren, damit man dem Vorwurf entgeht, man habe einen späteren Täter damit zur Anwendung anleiten wollen. Ferner ist dafür Sorge zu tragen, daß es demjenigen, der aus einem weitergebenen SOURCE-CODE schließlich das VirusProgramm generiert, nicht erspart bleibt, einen ausführlichen Hinweis auf die Gefährlichkeit des Programmes, sowie die Tatsache, daß der Autor ein Inverkehrbringen desselben ablehnt, zur Kenntnis zu nehmen."

Haftungsrechtliche Fragen

Eine der wichtigsten Fragen im Umgang mit Viren sind haftungsrechtliche Konsequenzen. Wir möchten hier nur einige Beispiele für denkbare Ansprüche der Opfer von Viren nennen und auf beweistechnische Probleme nicht weiter eingehen.
"Für Fehler (Bugs) in kommerziell verbreiteter Software haftet der Hersteller. Dieser Grundsatz deckt teilweise auch diejenigen Schäden ab, die durch die Anwendung grob fehlerhafter Programme entstehen. Selbstverständlich sind nur die Programmversionen von dieser Maxime gedeckt, die der Hersteller offiziell ausgeliefert hat. Demnach haftet der Hersteller schon dann nicht mehr in vollem Umfang, wenn der Anwender sich die Programme auf illegale Weise verschaft hat (Industriespionage, Softwarepiraterie) oder eine Version des Programms benutzt, die sich in der Struktur wesentlich vom ausgelieferten Orginal unterscheidet. Fazit: Keine Haftung des Herstellers bei Schäden durch 'verseuchte' Programme.
Der für die Verbreitung eines Virus Verantwortliche muß nicht nur für die Kosten aufkommen, die (wenn überhaupt möglich) die Wiederherstellung der Software erfordert, sondern auch für die durch die übrigen Aktivitäten des Virus entstandenen Schäden. Diese können die Schäden in der Software weit übersteigen, ja möglicherweise einen Umfang annehmen, den keine Privatperson mehr abdecken kann."

Strafrechtliche Aspekte

Das größte Problem für den Entwickler von Viren ist die strafrechtliche Relevanz seines Handelns. Das Entwickeln und anschließende Verbreiten eines Programmes ist solange nicht strafbar, wie sich keine Straftatbestände finden lassen. Da der Entwickler beim Virus am Schadenseintritt wiederholt mittelbar beteiligt ist, kommt hier Anstiftung oder Beihilfe zu den einschlägigen Straftaten in Betracht (allerdings bekanntlich mit derselben Strafdrohung, wie die Haupttat). Hier einige Leitsätze, die eine Hilfestellung geben können.
"Das Verhalten desjenigen, der einen Virus verbreitet (oder verbreiten läßt) ist dann strafbar, wenn er den Eintritt eines Schadens verursachen will. Eine Strafbarkeit ist auch dann anzunehmen, wenn der Schadenseintritt für wahrscheinlich gehalten und nichts zu dessen Abwendung unternommen wird. Problematischer ist der Fall, wenn ein Dritter, der die Virus-Routine erstmals vom Entwickler erhalten hat, sich entsprechend der ersten beiden Leitsätze strafbar macht. Hier könnte der Entwickler dann mit zur Verantwortung gezogen werden, wenn dieser mit der Reaktion des Dritten rechnen konnte.
Die Folgen des Einsatzes von ComputerViren sind unabsehbar und im Falle erfolgreicher Ermittlungen vom Verursacher zu tragen. Inwieweit der Entwickler zum Kreis der Verursacher zu rechnen ist, hängt vom Einzelfall ab; aufgrund seiner Kenntnisse obliegt ihm aber sicherlich eine besondere Sorgfaltspflicht."
Soweit einige Hinweise für experimentierfreudige Programmierer. Wer Viren vorsätzlich auf fremden Computern ohne Zustimmung des Eigentümers verbreitet, verstößt gegen eine Reihe von Gesetzen. Die strafrechtlichen Hinweise erscheinen uns unter Berücksichtigung der drohenden haftungsrechtlichen Ansprüche fast schon als sekundär.

Veröffentlichung von Computerviren

Mailboxbetreiber, die Viren in ihren Systemen zum Abruf anbieten, sollten die Diskussion im Brett "Rechtswesen" der CLINCH-Mailbox beachten. Dort werden weitere Hinweise auf die Problematik der Veröffentlichung von Viren gegeben.
"Eine Strafbarkeit (und zivilrechtliche Haftung) wegen der Veröffentlichung von Virusprogrammen unter dem Gesichtspunkt der Anstiftung zur Datenveränderung (etc.) sollte ausgeschlossen sein, wenn kein - auch versteckter - Vorschlag gemacht wird, dieses Programm ohne Einwilligung auf fremde Computer zu portieren. Zusätzlich würde ich sicherheitshalber empfehlen, ein Virusprogramm nur zusammen mit einer erkennbar ernstgemeinten Warnung vor den tatsächlichen und rechtlichen Folgen einer Portierung des lauffähigen Programmes zu veröffentlichen. Bei Beachtung dieser Empfehlung halte ich die Veröffentlichung von Virusprogrammen insoweit für (rechtlich) unbedenklich."
Wer mit Viren experimentiert, sollte sich der rechtlichen Konsequenzen bewußt sein. Nicht nur der höfliche, sondern auch der vorsichtige Mensch behält seine Viren daher vielleicht besser bei sich.

Teil 5

Ansichten und Einsichten der Diskussion im PC-Virenforum

"Ich verfluche den Tag, an dem ich mir eine Festplatte zugelegt habe!". Erste Reaktionen auf das Wissen um ComputerViren. Während im ersten Block des Virenforums hauptsächlich sachliche Informationen über ComputerViren vermittelt und von den Teilnehmern ergänzt wurden, war für den zweiten Teil eine Diskussion über die Folgen und den Umgang mit ComputerViren geplant.
Als die Bayrische Hackerpost im Frühjahr 1985 erstmals über Computerviren berichtete, stand die ComputerWoche Kopf und verglich Hacker mit der RAF. Eine Panikreaktion. Derartige Informationen aus solch einer Ecke sind wohl eher geeignet, kriminelle Potentiale zu entwickeln, war die Schluß"folgerung" der ComputerWoche. Das Unverständnis, dieses Thema zu bewältigen, führte zum Aufbau eines Feindbildes. Solchen Auswüchsen wollte sich der CCC in seiner Informationspolitik nicht aussetzen. Deshalb setzte schon Mitte '86 eine Diskussion über ethische Fragen beim Umgang mit ComputerViren ein. Ziel unserer Informationspolitik sollte nicht "Panikmache" oder das Heraufbeschwören einer Gefahr sein, sondern eine öffentliche Diskussion zur Vermittlung eines gesteigerten Unrechts- und Problembewußtseins. Der Chaos Communication Congress wurde als Forum bestimmt. Der Congress bietet eine Atmosphäre des Miteinanders, etwas, das auf kommerziellen Veranstaltungen unmöglich ist: offene Diskussion ohne Vorbehalte.

Im wesentlichen stellte sich die Frage: wie weit geht die Informationspolitik? Setzen wir uns bei der Veröffentlichung eines SOURCE-CODES dem Vorwurf aus, Bauanleitungen für logische Bomben zu verbreiten? In wieweit regen wir Nachahmungstäter an? Stellt schon eine detaillierte Veröffentlichung dieses Wissens eine Gefahr dar? Hier ergaben sich die unterschiedlichsten Betrachtungen.
Festzustellen war, daß Programmierer von ComputerViren mit ihrem Wissen bisher sehr verantwortungsvoll umgehen. Viele von ihnen fragen sich, was sie überhaupt damit machen sollen. Die Skrupel vor dem Vireneinsatz sind unterschiedlicher Natur. Ein Programmierer meinte: "Ich habe soviel Arbeit investiert, jetzt will ich auch sehen, was passiert" (auch die Atombombe mußte ausprobiert werden). Überwiegend sprachen die Congress-Teilnehmer sich gegen die bloße Veröffentlichung von Programmquellcode aus. Und wenn, dann nur mit eindeutigen Informationen über die Folgen und den Umgang mit ComputerViren. Einzelnen erschien schon die Beschreibung "überschreibender" und "nichtüberschreibender" Viren als zu detailliert. Fast durchgängig forderten die Teilnehmer eine offene Informationspolitik. Die freie Forschung im Sinne des "Free Flow Of Information Act" soll helfen, positive Ansätze zu entwickeln.
"Veranstaltungen wie der CCC'86 erzeugen keine entscheidende Veränderung beim Umgang mit Computern. Sie vermitteln eher ein Bewußtsein von der Tragweite des Handelns" formulierte ein Teilnehmer. Bisher wird, was ComputerViren betrifft, der Kreis der "Informierten" noch als sehr klein eingeschätzt. Daß detaillierte Informationen über ComputerViren Nachahmungstäter anlocken, muß in Kauf genommen werden, wenn der schleichenden Entwicklung entgegengearbeitet werden soll. Die Geschichte hat gezeigt, wie gefährlich es ist, Sicherheitsfragen von der offenen Diskussion unter Fachleuten auszunehmen. Die Affäre um Sicherheit oder Unsicherheit des Geheimcodes der deutschen Führung im zweiten Welktkrieg ist als abschreckendes Beispiel oft genug erwähnt worden. Vielmehr erwarten Congressteilnehmer die Einleitung einer öffentlichen Diskussion über die "Restrisiken" neuer Technologien. Gerade die Popularität des CCC, der seit jeher technikkritische Themen erörtert, soll helfen, dieses Thema einer offenen Diskussion zuzuführen.
Erstaunlich waren Thesen über "WiderstandsViren". So sahen einige Congressteilnehmer in ComputerViren ein legitimes Mittel zum Volkswiderstand gegen unmenschliche, zentralisierte Grossrechenzentren. Auch deuten einige Hinweise aus der Scene auf einen Virusangriff gegen die Volkszählung hin. Parallelen zum Science Fiction-Roman "Der Schockwellenreiter", in dem John Brunner (Heyne SF 3667) schon 1975 das Bild einer computerabhängigen Welt zeichnete, die durch ein "Wurmprogramm" befreit wird, sind erkennbar.
Frankreich entschied sich im Gegensatz zur BRD bewußt gegen die Einführung eines maschinenlesbaren Ausweises. Der Grund: Demokratische Systeme benötigen einen Spielraum, der Widerstand gegen diktatorisches Takeover ermöglicht. So wurde die Forderung laut, dieses technisch spezialisierte "Herrschaftswissen" auch als "WiderstandsWissen" zu fördern. Dem entgegen stand der überwiegende Teil der Besucher mit der Auffassung, daß Hacker sich nicht außerhalb der Gesetze stellen wollen, sondern eher einen Spielraum ausnutzen, um auf Gefahren aufmerksam zu machen.
Weitgehend unberücksichtigt blieb in den Diskussionen das Potential krimineller Kräfte, die sich Vorteile durch den Einsatz von Viren verschaffen könnten. Weiterhin dürfen politische Gegner, sowie Geheimdienste und terroristische Gruppen bei der Gefahrenabschätzung nicht vergessen werden. Wo ökonomische oder ideologische Beweggründe vorliegen, ist die Gefahr einer VirusAttacke weitaus wahrscheinlicher als aus den Reihen der privaten Computeranwender. Diese handeln viel eher verantwortungsbewußt.
So wurden Forderungen laut, daß ComputerSysteme, die personenbezogene Daten verarbeiten oder hochkritische Steuerfunktionen (zB. in Atomkraftwerken) übernehmen, absolut virensicher sein müssen. Andernfalls darf man derartige Aufgaben nicht solchen anfälligen Technologien überantworten. Weiterhin muß eine ethische Barriere gegen den Computermißbrauch, aber auch gegen den fahrlässigen Computergebrauch aufgebaut werden. Folgend sollen Forschungsergebnisse die Entwicklung von Abwehrmechanismen ermöglichen. Die Erhöhung der "Risikoschwelle" (schnellere Entdeckung) ist jedoch nur eine technische Hilfe, die weiterhin ein "Restrisiko" aufweist.
"Das Problem sind nicht die ComputerViren, sondern die Katastrophen, die durch die Abhängigkeit von Technologien entstehen", so die Schlußfolgerung eines Congress-Teilnehmers. Nach Jahren bedenkenloser Technologiegläubigkeit forderten die ersten technischen Mega-Katastrophen (Bhopal, Tschernobyl, Basel) ihre Opfer. Der CCC fordert seit langem eine sozialverträgliche Gestaltung von Technologien. Die unverträgliche Verbraucherhaftung bei Mißbrauch von Bildschirmtext oder Euroscheckkarten waren einige kritische Ansätze aus der letzten Zeit. Die ComputerViren stellen nun eine neue, äußerst brisante Erscheinung im Kräftespiel moderner Techniken dar. Wissenschaftler erörtern seit einiger Zeit "The Ultimate Error Message", den Weltkrieg durch einen Computerfehler.
Die Aufarbeitung des CCCongress'86 anhand einer Videodokumentation zeigt bisher unerörterte Bereiche auf. Die Redaktion geht davon aus, daß in den nächsten Monaten weiteres Material über ComputerViren veröffentlicht wird.
Der CCC veranstaltet daher am 18. und 19.April '87 ein weiteres VirenForum. Ein Anmeldeformular erscheint in der DATENSCHLEUDER 19. (Zum April wird auch die Videodokumentation über den CCC'86 fertiggestellt sein.)
LS23

"It's the Defense Department. They're calling around the neighborhood to see if anyone can help them figure out why every one of their missiles keeps overriding their commands and aiming themselves at Mrs. O'Reilly's house down the block."

Für eine Handvoll Daten

De-Anonymisierung des gezählten Volkes

Es begab sich aber zu der Zeit, daß ein Gebot ausging von dem Kaiser Augustus, daß alle Welt sich schätzen ließe (Chaos-Textbaustein 42).
So wurde zu biblischen Zeiten die Tatsache dokumentiert, daß jede Regierungsform Informationen über die Regierten benötigt, also Daten, anhand derer man Entscheidungen für die Zukunft treffen kann. Dieses legitime Bedürfnis findet sich heutzutage wesentlich prosaischer formuliert im Volkszählungsgesetz wieder. Indula (Textbaustein aus dem CDU-Textsystem; bedeutet 'in diesem unseren Lande') werden traditionell Erhebungen durchgeführt, die aufschlußreiche Daten zur Befriedigung des Informationshungers der Behörden und der Wirtschaft liefern sollen. Bekanntlich wurde - nach großen öffentlichen Protesten - die ursprünglich für 1983 vorgesehene Volkszählung durch ein Urteil des Bundesverfassungsgerichtes gestoppt und den Verantwortlichen eindringlich klargemacht, zu welchen Bedingungen eine künftige Zählung machbar sei:
Es sei zu "prüfen, ob eine Totalerhebung trotz einer inzwischen fortgeschrittenen Entwicklung der statistischen und sozialwissenschaftlichen Methoden noch verhältnismäßig ist" (BVerfG'83, Seite 59). Darüber hinaus bedürfe es einer "möglichst frühzeitigen, faktischen Anonymisierung, verbunden mit Vorkehrungen gegen eine Deanonymisierung" (BVerfG'83, S. 52/53). Interessant ist die Forderung des Gerichtes nach öffentlicher sachlicher Information auch über die Art der statistischen Datenverarbeitung, "da Abschottung statt Information zu Mißtrauen und mangelnder Kooperationsbereitschaft führen würde" (BVerfG'83, S. 54)
Jetzt stellt sich natürlich die Frage, was der CCC mit der ganzen Sache zu tun hat. Nun, erstens interessiert die Redaktion von vornherein alles, was irgendwie nach Mißbrauch von Macht mittels des Werkzeugs Computer riecht. Zweitens ist so ein Urteil des Bundesverfassungsgerichtes ja ganz nett, aber wenn die Kontrollinstanzen fehlen, welche die Durchführung eines solchen Urteils überwachen, ist Jedermann aufgerufen, das Seine dazuzutun, um Schaden von diesem unseren Volke abzuwenden. Drittens haben wir im Rahmen des Chaos Communication Congress 1986 Material erhalten, das uns geradezu verpflichtet, tätig zu werden.
Am Institut für Informatik der Universität Hamburg wurden in den letzten Monaten umfangreiche Studien durchgeführt, die zweifelsfrei belegen, daß die mit der Volkszählung 1987 gewonnen Daten, entgegen der eindeutigen Forderung des Verfassungsgerichtes, eben nicht 'faktisch anonym' sind, sondern sehr wohl, und recht einfach, eine Identifizierung des Dateninhabers ermöglichen. Den - wahrscheinlich neuen - Begriff des DATENINHABERS benutzen wir hier sehr bewußt, um deutlich zu machen, daß es in einer Informationsgesellschaft auch ein Grundrecht auf informationelle Selbstbestimmung geben muß. Und das fängt eben damit an, daß jeder Einzelne selbst bestimmt, wer welche Daten über ihn sammelt und benutzt.
Die unter der Leitung von Professor Klaus Brunnstein durchgeführten Versuche zeigen erschreckend deutlich, mit welch einfachen Mitteln es möglich ist, aus den angeblich anonymisierten, d. h. nicht mehr personenbezogenen Daten wieder personalisierte Daten zu machen. Grundlage der Versuche war eine künstliche Volkszählungsdatei, die ausschließlich Daten enthält, wie sie bei der Zählung 1987 anfallen werden, ohne die momentan laufende Stammdatenerhebung bei den Hausbesitzern und Arbeitgebern auch nur annähernd einzubeziehen, so daß letztlich die Angaben, die jeder einzelne von uns macht, es ermöglichen, wieder auf jeden Einzelnen zu schließen.
Brunnsteins Studie zeigt einwandfrei, daß es mit einem einfachen Werkzeug, wie dem Datenbanksystem DBase III unter MS-Dos, möglich ist, mit wenigen Filtervorgängen ganz konkrete Einzelpersonen aus einem Datenberg von 100 000 Datensätzen herauszufischen. Bei 60 Millionen Datensätzen braucht man halt nur eine größere Festplatte und entsprechend mehr Zeit...
Wir wollen die Vorgehensweise zur Reanonymisierung von Volkszählungsdaten anhand eines Beispiels deutlich machen: Zielgruppe des Versuchs sind 46-jährige Männer aus der Bürobranche. Unser erster Schritt ist also konsequenterweise der, zuerst nach dem Geburtsjahr zu filtern. Es bleibt eine Datei mit 915 Personen übrig, die 1940 nach dem Stichtag der Volkszählung geboren wurden. Diese Datei filtern wir nach dem Geschlecht und erhalten eine Datei mit 443 Personen, die wir auf das Merkmal Erwerbstätigkeit prüfen. Übrig bleiben 386 männliche Erwerbstätige von 46 Jahren. Bürokräfte haben die Schlüsselnummer 78, also suchen wir jetzt danach und erhalten eine Datei, die nur noch 26 Personen enthält. Wir

sollten uns dabei deutlich vor Augen halten, daß wir nur drei Merkmale brauchten, um aus 100 000 Datensätzen einige wenige herauszufischen. Der nächste Schritt besteht darin, die 'Wirtschaftsabteilung' zu sondieren. Wir erhalten elf Datensätze, die wir auf das Merkmal Schulabschluß prüfen. Ergebnis: fünf Volks- bzw. Realschüler. Zusätzlich fragen wir, wer davon einen Berufsfachschulabschluß hat, übrig bleiben drei Kandidaten.
Wir haben bislang erst sechs signifikante Merkmale untersucht, werden aber trotzdem hinterhältig und fragen uns: was wissen wir denn sonst so über die Drei? Über das Merkmal 'gemeinsamer Haushalt' können wir weitere Schlüsse ziehen (Das Volkszählungsgesetz 1987 schreibt ausdrücklich vor, daß "die Zusammenhänge zwischen Personen und Haushalt, Haushalt und Wohnung, Wohnung und Gebäude . . . festgehalten" werden, was beim Gesetz zu Zählung '83 nicht der Fall war). Wir könnten nun also noch feststellen, daß Herr A ledig und religionslos ist und in einem Einzelhaushalt lebt. Damit ist er nun aber wirklich eindeutig reanonymisiert, denn B und C sind verheiratet und über ihre Ehepartner eher noch leichter reanonymisierbar. Zusammen mit der Tatsache, daß auch eine Information vorhanden ist, anhand derer der sogenannte Block des Dateninhabers feststellbar ist (Blöcke sind die kleinste Einheit von Datensatzmengen. Sie begrenzen die Datensätze von Personen, die in einer Straßenfront zwischen zwei Einmündungen von Nebenstraßen wohnen), wird nun leicht vorstellbar, warum Herr A spätestens 1989 Werbung von einem Heiratsvermittler bekommt, während Herr B davon verschont bleibt.
Der Forderung des Bundesverfassungsgerichts wird also mit der Volkszählung 1987 in keiner Weise Rechnung getragen. Faktische Anonymisierung bedeutet nunmal, daß eine Reanonymisierung nur mit unverhältnismäßig hohem Aufwand möglich sein darf. Schon durch die Art der erhobenen Daten wird eine Entscheidung, die unsere höchste verfassungsmäßige Instanz getroffen hat, schlicht ignoriert. Abschließend noch einige Zitate aus der Studie, die wir unkommentiert lassen, da sie für sich sprechen:
"Bei diesen Ergebnissen ist zu berücksichtigen, daß wesentliche Merkmale der Volkszählung, die eine Identifizierung noch erleichtern, etwa die Adresse des Arbeitgebers oder der Ausbildungsstätte, in den Re-Identifizierungs-Versuchen nicht einmal benutzt wurden."
"Erstens: Es gibt kaum Personen innerhalb des Datenbestandes, die nicht anhand der über sie gespeicherten Merkmale re- identifizierbar wären.
Zweitens: Mehr als die Hälfte aller Erwerbstätigen können schon mit wenigen Merkmalen . . . re-identifiziert werden" ". . .da die Organisation der Statistik als interne Aufgabe der Exekutive angesehen wird, gibt es praktisch keine Kontrollinstanz. . ."
"So sind die Präsidenten der Statistischen Ämter die letzten wahren, weil unkontrollierten Könige dieser Republik."
Alle Zitate und das Re-Identifizierungsbeispiel stammen aus: "Mitteilung Nr. XX über Möglichkeiten der Re-Identifikation von Personen aus Volkszählungsdaten" von Klaus Brunnstein, Hamburg; Dezember 1986.
(Die Studie sowie Beispieldaten und die Re-Idenfikationsprogramme können über die DATENSCHLEUDER-Redaktion bezogen werden).

goblin

KLEINanzeige

Dirk aus Berlin, der an der Diskussion Samstag Nacht auf dem CCCongress teilgenommen hat: die Moderatorin möchte Dich treffen. Bitte hinterlass Deine Tel-Nr. für Ingrid beim AL-Buero 861 4449.

aus: 52↑ Bereitschaftspolizei - heute — 12/86

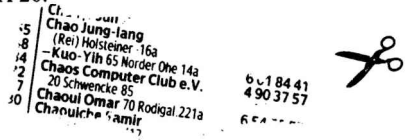
Radio Bremen ist auf dem CCCongress'86 eine Videocassette (Umatic) abhanden gekommen. Erkennungsmerkmal: Kassette ist zu groß für VHS-Rekorder. Mögliche Finder bitte während der öffentlichen Chaosdienstzeiten Di-Do 12-15 unter 040-490 37 57 melden.

Hackersets

— Anzeige —

(So lange der Vorrat reicht)

CPM-Portable EPSON PX8, 64 KB, Microcassette, Display 80★11, mit Akku und Garantie aus Sonderposten DM 870,- für CCC-Mitglieder (notfalls gleichzeitig beantragen)
Versand erfolgt als Wertpaket nach Eingang eines V-Schecks an den CCC, LS PX8, Schwenckestr. 85, 2000 HH 20.



IMPRESSUM

Die Datenschleuder Numero 18
Das wissenschaftliche Fachblatt für Datenreisende
D-2000 Hamburg 20 Schwenckestrasse 85

Geonet : Geo1:Chaos-Team
Btx : *655321#
Herausgeber und ViSdPG:
Herwart Holland-Moritz
Mitarbeiter (u.a.): R. Schrutzki, S. Wernery, A. Eichler, P. Franck, H. Gruel, M. Kuehn, Esco, Andy M.-M., S. Stahl, padeluun, KS, jwi, D. Wintschnig, Poetronic; Rhein/Main: Erich Engelter sowie die ungenannten Geheimnisträger.

Vielfarb-Kartoffeleigendruck im Selbstverlag.
Februar 1987 - Made in Eile

WIKG

2. WIrtschaftsKriminalitätsGesetz

Da das 2.Wirtschaftskriminalitätsgesetz (WIKG) zum ersten August'86 in Kraft trat, war es natürlich Gesprächsgegenstand eines CCCongress-Workshops. Unter Leitung des BHP'lers Sponti wurde über die Auswirkungen und die Zukunft der Hacker diskutiert. Einig war man sich, daß NUI-Mißbrauch als "Täuschung im Datenverkehr" strafbar, und es noch unklar ist, wo die Grenze zu ziehen ist zwischen Daten, welche legal abgerufen werden können, und denen, welche nicht legal abrufbar sind.
Ist beispielsweise das Prompt, oder die Meldung, um wessen System es sich handelt, bereits sicherheitsrelevant? Ist eine normale ID & Paßwort-Sperre bereits als "besonderer Schutz" zu verstehen? Wichtig auch die Information, daß die ALTOS-Box jedes Einloggen und Ausloggen als Vorgang mit allen dabei anfallenden Daten protokolliert, bislang nur zur Ausmerzung von Software-Bugs, in Zukunft aber - mit Zustimmung der Firma ALTOS, der wohl nichts anderes übrig blieb - auf Veranlassung der Behörden, nachdem eine Rückverfolgung stattfand, bei der sich jemand mit einer Leih-NUI bei ALTOS eingeloggt hatte.
Um die Argumentation der Juristen und die Auswirkungen und - legungen des 2.WIKG genauer kennenzulernen, bitten wir jeden, der aufgrund des 2.WIKG in Schwierigkeiten gerät, sich bei uns zu melden, damit wir uns informieren können.
Auf der Veranstaltunfg wurde auch die Auffassung vertreten, daß die Hacker - als kleine Fische - Studien- und Übungsobjekte der LKA's sind, die daran Erfahrungen sammeln für die Bekämpfung wirklicher Wirtschaftskrimineller. Derzeitiger Stand der Dinge sei zwar, daß die meisten Ermittlungsbeamten bei Hausdurchsuchungen wenig bis gar keine Ahnung hätten (so kam es vor, daß leere Diskettenhüllen und -schachteln mitgenommen wurden), daß aber die Beamten in den LKA's, die dann den Fall weiterbearbeiten, sehr wohl wissen, was sie tun. Man sollte also nicht auf deren Unkenntnis setzen!

Ls 111

Schön wär's

Falschgeld in TEMPO

Daß der CCC für die PARLAKOM-Studie vom Bundestag 38.000 DM erhalten habe, wie die Zeitschrift TEMPO es darstellte, ist leider eine Ente. Zur Sanierung der Clubfinanzen wäre die Summe durchaus hilfreich. Das Foto zu dem TEMPO-Artikel (ohne Unterschrift und Quelle) zeigt auch nicht die ISDN-Baustelle im Bundestag, sondern die bewährte Telefonzentrale des Chaos Communication Congress. Ferner ist richtigzustellen: Bei der Erarbeitung der Studie waren "nur" Leute aus dem CCC und dem Arbeitskreis Politisches Computern (APOC) beteiligt, die eine mögliche Computer-Wende der Grünen geistigmoralisch zu unterstützen versuchten. (Die Studie kann von der DS-Redaktion bezogen werden).

ls5

Wirtschaftsspionage

British Telecom Is Watching You

München (bhp/ds) - Vertrauliche geschäftliche Informationen über europäische Industriefirmen, erlangt durch Überwachungszentren der US-Amerikanischen Streitkräfte in Europa, werden an konkurrierende Firmen in den USA übermittelt. Dies geht aus einem kürzlich veröffentlichen Buch zu diesem Thema hervor.
Der Verfasser, ein früherer Mitarbeiter der US-Luftwaffe, beschreibt darin, wie die Telekommunikation in mehreren Staaten der Europäischen Gemeinschaft überwacht wird und wie den US-Firmen fertig aufbereitete Informationen zugänglich gemacht werden. Dieser Teil der Überwachung überwiegt demnach bei weitem das Abhören des sowjetischen Militärfunkverkehrs, beschreibt Duncan Campbell in seinem Buch "The Unsinkable Aircraft Carrier" (der unsinkbare Flugzeugträger; d. Übers.). Tom Litterick, Abgeordneter des britischen Parlaments, beschuldigte daraufhin die Vereinigten Staaten der "Wirtschaftsspionage".
"Die wichtigste Station für die gegenseitige Sicherheit in der Welt", so ein früherer Direktor der US National Security Agency, liegt in Menwith Hill in der Grafschaft Yorkshire, Großbritannien. Einige 10.000 Telefonleitungen laufen dort zu der nahegelegenen Relaisstation der britischen Telefongesellschaft British Telecom. Menwith Hill wird außerdem durch einen Hohlleiter versorgt, der bereits vor seiner Modernisierung vor zwei Jahren eine Kapazität von 32.000 Telefongesprächen gleichzeitig hatte. Großbritannien ist einer der Hauptzugänge für Datenleitungen von Ost- und Westeuropa nach Afrika sowie Nord- und Südamerika. Die "Spezialität" der Station in Menwith ist das Anzapfen der fest gemieteten Standleitungen der europäischen Postverwaltungen.
Nahezu der gesamte internationale Datenverkehr, Nachrichten, Telegramme und Telefongespräche von Firmen, staatlichen Institutionen, der über Großbritannien läuft, wird überwacht und ausgewertet. Die Mehrzahl der ausgewerteten Informationen werden an das Hauptquartier der NSA in Fort Meade, USA, weitergeleitet.
Europas schwache Position in diesem Spiel wird noch zusätzlich verdeutlicht durch den Kommentar eines Amerikaners zu diesem Thema: "Nicht einmal wenn sie wollten, könnten die Verbündeten davor sicher sein. Sie arbeiten alle mit Geräten, die sie von uns bezogen haben."

Aus: I'M, Information Market, Ausgabe 46, Dec. 1986 - Feb. 1987
Hrsg.: Commission of the European Communities.
ds-Abdruck mit freundlicher Genehmigung der BHP.

Real Hacking

Bombenstimmung beim CCC'87

Ein Kameramann von Radio Bremen - er sucht hinter einem Elektrokasten mühsam Deckung - steht im nieselnden Schneematsch und betet: "Lieber Gott, mach bitte, daß sie hochgeht. Bitte, lieber Gott, ich werde mir auch einen zweiten TAZ-Aufkleber auf die Kamera kleben."
Er ward nicht erhört.
Mitten in der großen VIRUS-Diskussion während des CCCongresses hatte ein Unbekannter in REAL HACKING-Manier einen Virus eingeschleust: telefonisch gab er bekannt, daß jeden Augenblick eine BOMBE hochgehen würde. Von Anfang an der Lacher des Abends. Das Haus wurde aus juristischen Gründen mal eben kurz geräumt, das Chaos-Team durchkämmte mit einem Mienensuchroboter (20 cm hoch, ferngesteuert, bei Karstadt für 35 Mark) den zweiten Stock. Kleinere Aufregung bei der Räumaktion gab es erst, als ein heimlicher Verbündeter des Anrufers - ebenfalls in REAL HACKING-Manier - ein bis zwei Luftballons explodieren ließ. - Was haben wir uns alle erschrocken.
Draußen im Regen gings dann ab. In ausreichendem Sicherheitsabstand von zwei Metern zum Eidelstedter Bürgerhaus begannen sich Trüppchen zu bilden und ihre Ansichten zur Virusfrage mit harten Bandagen auszutauschen. Endlich war die trennende Stuhlreihen- und Bühnensituation überwunden. Hier brachen die wohlhabenden Peripherie-Besitzer weinend zusammen: "Ich will keinen Virus auf meiner Festplatte", während bescheidene Equipmentbesitzer triumphierten, daß der Virus ihrer Datasette (schon wieder ein Riesenlacher) kaum etwas anhaben könne.
Der Sicherheitsabstand zum Haus schrumpfte auf 50 Zentimeter. Die Kripo hatte die Bombendrohung nicht ernst genommen, aber aus technischen Gründen sollten erst noch einmal alle draußen warten. Kurz danach ging das Gerücht um, daß sich der Chaos-Helfer an der Lautsprecheranlage derart in Panik geschrien hätte, daß er erst nach einigen kräftigen Ohrfeigen aufhörte, "Hilfe, Panik, alle raus!" zu schreien. Er hatte anschließend das gesündeste Aussehen von allen (rote Bäckchen. . .).
Das Frösteln wurde langsam unangenehm und jeder versuchte, sich warmzureden. Zum 100sten Mal wurde der Satz des Tages zitiert: Ich bin nicht gegen Gesetze, ich lasse sie nur außer acht. Darauf aufbauend, versuchten die Hintersten zuerst, in das warme Haus vorzudringen. Einige versuchten reinzukommen, indem sie sich (Real Hacking!) als Chaos-Dienst ausgaben, hatten aber nicht mit dem Real Serum (sprich ECHTEM Chaos-Dienstler) an der Tür gerechnet. Drin explodierte ein weiterer Luftballuun (sind wirklich wie Zeitbomben; sie finden ihre scharfe Ecke von alleine) und endlich gab Asterix die Tür wieder frei.
Der Kameramann (ein besonders guter Mensch, weil er ja einen TAZ- Aufkleber auf der Kamera hatte) war ein wenig traurig. Live- Explosionen lassen sich nämlich immer ganz prima an die Tagesschau verkaufen (je mehr Tote, desto besser. . .). Aber da er ja kein Zyniker ist, war er natürlich auch ein bißchen erleichtert.
Dies war ein Beitrag über Bombendrohungen. Und über REAL HACKING. Über Viren steht hier nichts.
Weiterblättern.

padeluun

BiFu

Bild und Funk auf dem CCC'86

Wie in jedem Jahr auf dem Chaos Comunication Congress waren die Funkamateure wieder mit Bild und Funk vertreten. Schwerpunkte wie Packet Radio wurden in vorausgegangenen DATENSCHLEUDERN ausführlich abgehandelt.
Erstmals auf einem CCCongress war die Amateurfunkfernseh- Empfangsanlage (ATV-Anlage), die von DL1HK zur Verfügung gestellt worden war. Im wesentlichen besteht sowas aus einer Antenne für das 23 cm-Band, einem Converter, der die Signale ins normale TV-Band umsetzt und einem Fernseher mit Kabeltuner. Mit dieser Mimik gelang es (trotz schlechter Antennenlage), ein verwertbares Farbbild vom ATV-Relais (Sendeleistung nur ca. 30 Watt) auf den Screen zu bekommen. Dazu war nichtmal ein Composter nötig!
Wenn kein Amateur über das Relais arbeitet, sendet es automatisch einen aktuellen Ausschnitt vom Meteosat-2-Wetterbild im Wechsel mit einem Testbild oder einem Außenbild einer Kamera, die beim Relais angebracht ist.
Der eigentliche Witz des Relais liegt darin, daß auch ein Amateur, der selbst keine Bildübertragung machen kann, sich mit einem 70 cm-Funkgerät auf den Tonträger aufschalten und so seine Kommentare zu den gezeigten Bildern abgeben kann. DC1XI war so frei, während der Veranstaltung als Ansprechpartner zu dienen und sozusagen auf Abruf eine Stationsbeschreibung (im Hackcenter herrscht gegen den Kabelsalat richtig Ordnung) live einzuspielen oder Amateur-Videotapes zu senden. Krieg der Sterne zeigen ist zwar ohne weiteres machbar, aber nicht erlaubt (AFuG, (c) und so).
Für den CCC'87 hat DC1XI in Aussicht gestellt, entweder vom Congress live zu senden (so die Technik will), oder aber kurze Tapes von zu Hause einzuspielen. Mal sehen ob's klappt - frei nach dem Motto: Hier ist (DL0)CCC mit eigenem TV-Programm.

Quartierisch

Abenteuerurlaub in der Hafenstraße

Zu Verwicklungen kam es bei der Organisation der Übernachtungsmöglichkeiten für den CCC'86. Da die ursprünglich vorgesehenen Räumlichkeiten des CVJM nicht mehr mietbar waren, wurde die städtische Wohnungsverwaltung SAGA angerufen. Das Telefonat, sinngemäß: "Der CCC bräuchte für einige seiner vorwiegend jugendlichen Gäste Übernachtungsplätze. Da die geplante Unterbringung nicht möglich ist, dachten wir daran, unseren CongressTeilnehmerInnen ein anderes Stück Hamburg zu zeigen, eine Art Kurzabenteuerurlaub. In Ihren Häusern an der Hafenstraße stehen ja zumindest vier Wohnungen leer, die kürzlich geräumt wurden. Für die Dauer des Congresses würden wir gern ein paar unserer Gäste in der Hafenstraße einquartieren. Da der Congress nur zwei Tage dauert, ist mit Räumungsproblemen nicht zu rechnen."
Die Absage bestand aus einer Unbewohnbarkeitserklärung. Daraufhin wurde die Jugendherberge am Hafen angesprochen; ein Dank für die Unterstützung, die den Gästen dort zuteil wurde.

wau

NetzWorkShop Ein Resümee

In einer nächtlichen Sitzung trafen sich rund 30 TeilnehmerInnen des CCC'86 zu einem Workshop, um Realisierungsmöglichkeiten alternativer Computertechnik und offener Netze zu besprechen.
Als ein gelungenes Beispiel wurde die Berichterstattung der Bayrischen Hackerpost (B.H.P) gewertet. Die B.H.P. hatte bereits zwei Tage nach dem atomaren Katastrophe in Tschernobyl aktuelle Meßdaten über den Verstrahlungsgrad in Teilen der Bundesrepublik durch die Mailboxen-Szene geschickt. Darüber hinaus wurden Hintergrundberichte angeboten, die die Bedeutung von Fachbegriffen und Meßgrößen erläuterten.

Praxis in der Erprobung

Die Grenzen der elektronischen Kommunikation sahen die meisten Teilnehmer zunächst bei den relativ hohen Kommunikationskosten. Eine Situation, die sich durch die Erhöhung der Benutzergebühren für Datex-P noch verschärfen wird. Einer der Teilnehmer fühlte sich unter einem "Haufen Fachidioten", die über Perspektiven sprechen, an denen er aus finanziellen Gründen nicht teilhaben kann. Auch vor diesem Hintergrund wurde die Notwendigkeit betont, lokale Mailboxen, die von Privat betrieben werden, inhaltlich und strukturell zu unterstützen.
Versuche in dieser Richtung werden derzeit mit der Hamburger C.L.I.N.C.H.-Box angegangen. Seit Sommer 1986 betreibt CCC- Mitglied Reinhard Schrutzki eine Mailbox, die trotz einiger Mängel für inhaltliche Arbeit geeignet erscheint. Die C.L.I.N.C.H.-Box dient derzeit den Redaktionen des Genethischen Informationsdienstes und der DATENSCHLEUDER als "hauseigener Nachrichten-Vermittlungsrechner". Der Arbeitskreis für politische Computeranwendung (APOC) wickelt über diese Box Koordinierungsaufgaben ab und bietet im Brett "Politik" Kurznachrichten zu aktuellen Entwicklungen aus dem Bereich alternative Computeranwendung an.
Auf größeres Interesse stößt auch das Brett "Forum". Das für inhaltliche Diskussionen eingerichtete Brett bezieht sich derzeit überwiegend auf Themen aus dem Umfeld des CCC. Immerhin konnte an einem kleinen Beispiel demonstriert werden, was Mailboxen in der Praxis leisten können. Mitglieder der APOC hatten eine Diskussion über die Passfotos und Sicherheitskärtchen auf dem Kongress angezettelt. Sie kritisierten, daß alle Besucher verpflichtet wurden, solche an den Überwachungsstaat erinnernde Ausweise zu tragen. Sie schlugen vor, daß Besuchern lediglich ein Eintrittsstempel verpaßt wird, vergleichbar mit dem Verfahren "jeder mittelmäßigen Disko". Dieser Vorschlag wurde schließlich praktiziert. Der Prozess der Entscheidungsfindung, schriftlich dokumentiert, konnte während des Kongresses nachgelesen werden.

Elektronischer Schnellfick

Wau Holland machte während des Workshops deutlich, daß sich durch die Schnelligkeit des Mediums bereits im kleinen Kreis neue Informations- und Entscheidungseliten herausbilden.
Darüberhinaus brächten Mailboxen auch Informationsüberflutung sowie Beschleunigung, Verflachung und Ver-Rechtlichung zwischenmenschlicher Beziehungen hin zum elektronischem Schnellfick.

Wer deshalb oder anderen Gründen nicht am "elektronischen Vertrauenskreis" teilnehmen könne oder wolle, sei von Entscheidungsprozessen abgeschnitten. Kritisch würde diese Situation vor allem, wenn innerhalb der Boxen Diskussionen über Personen oder soziale Strukturen entstehen, ohne den direkt oder indirekt davon Betroffenen die bislang üblichen Möglichkeiten zur Reaktion zu gewähren.
Die neue Qualität der Mailbox sei unter anderem ihre Zwitter-Rolle als privates und gleichzeitig öffentliches Informationssystem. Zudem sind seien einerseits so flüchtig wie Radiowellen, andererseits als Papierdokumente (Ausdrucke) archivierbar.
Die Praxis zeige, wie wichtig es ist, die Konsequenzen verbreiteter Informationen zu bedenken. Es stelle sich immer wieder die Frage, welche Informationen, zu welchem Zweck, wann an wen wie und über welchen Informationsweg weitergegeben werden.
Jürgen Wieckmann wertete die Aktivitäten auf der C.L.I.N.C.H.-Box als längst überfälligen Experimentierraum, der "uns endlich die Möglichkeit gibt, unsere theoretischen Vorstellungen anhand der Praxis zu überprüfen und weiterzuentwickeln."

Voraussetzungen für Perspektiven

Mehrfach kam die Anregung, vergleichbar mit den Viodeoläden der 70er Jahre Computerläden aufzubauen, die eine praxisorientierte, alternative Computeranwendung erproben sollen. Aufgabe dieser Computerläden sei unter anderem, anwenderorientiertes Wissen zu vermitteln und Interessenten anhand referierbarer Projekte dazu zu befähigen, das Medium zur Umsetzung eigener Interessen sachgerecht einschätzen zu können. Darüber hinaus gelte es, das Wissen über Informationsverbreitung und Informationsbeschaffung als kulturelle und politische Aufgabe zu begreifen.
Die Computerläden hätten vor allem die Aufgabe, inhaltliche Arbeit bestehender Gruppen durch Computertechnik zu stärken und dabei auch die medienspezifische Eigenheiten des Computers im positiven Sinne zu nutzen. So habe die Videoszene eine Videokultur hervorgebracht, die neue Sehformen, Produktionsweisen und Bildgestaltungen hervorgebracht habe. Ein solcher Ansatz fehle der Computerszene bisher völlig.
Im Februar wird es im Rahmen einer Zukunftswerkstatt ein Treffen interessierter Kreise geben (siehe Termine an anderer Stelle im Heft), die ergebnisorientierte Konzepte zu solchen Ideen erarbeiten und vorstellen wollen. Diese Konzepte sollen auch Grundlage sein, um Anlauffinanzierungen durch die öffentliche Hand zu beantragen. jwi/(ls5)

Bestellfetzen (Bei Bedarf abbeissen und ausgefüllt einschicken (am besten an uns))

Jajajajaaa- ich möchte versuchen, die folgenden Sachen von Euch zu bekommen:

Wieviel ?	Einzelpreis	Was ?
	20.00 DM	Einmalige Aufnahmegebühr für den Chaos Computer Club
	60.00 DM	Mitgliedschaft im CCC für ein Jahr für Schüler, Studenten und ähnliches
	120.00 DM	Mitgliedschaft im CCC für ein Jahr für Normaluser
	230.00 DM	Ich will mehr: fördernde Mitgliedschaft im CCC für ein Jahr
	2.50 DM	Probeexemplar der DATENSCHLEUDER, frankierten Rückumschlag beilegen
	30.00 DM	Sozialabo der Datenschleuder für ein Jahr (Schüler, pipapo)
	60.00 DM	Standardabo der Datenschleuder für ein Jahr
	120.00 DM	Ich will mehr (bezahlen) : Förderabo der Datenschleuder für ein Jahr
	3.33 DM	10 Aufbacker 'Kabelsalat ist gesund' , Standardausführung
	3.33 DM	1 Din A4 - Bogen Aufbacker 'Achtung Abhörgefahr', ungeschnitten, postgelb
	25.00 DM	Infopaket 1: Computerviren 1 MS-Dos Disk 170k mit Demovirus und munteren 100kB Dokumentation zum Thema Viren
	25.00 DM	Infopaket 2 : Volkszählung & Reidentifikation 2 MS-Dos Disks 170k mit Beispieldaten (künstliche Bürger) , DBaselll - Programmen zur Reidentifikation und 17 Seiten Gebrauchsanweisung
	?.?? DM	Porto, Verpackung, Trinkgeld, Bussgeld , Spenden etc
		Summe:

Die Kohle liegt bei als : Briefmarken <= 0.80 DM V-Scheck Blankoscheck (lechz) Bar

(Zutreffendes markieren, Nichtzutreffendes löschen, oder sonstwas)

Nur für zukünftige Mitglieder:

Ich zahle meine Mitgliedsbeiträge jährlich halbjährlich vierteljährlich stündlich

und zwar bar per V-Scheck Überweisung

Ihr dürft abbuchen (Einzugserlaubnis liegt bei)

Überweisungen bitte an : Postgirosamt Hamburg, 59 90 90 - 201 , Chaos Computer Club e.V., Hamburg

Nur für zukünftige Mailboxbenutzer:

Ich will Benutzer der CLINCH - Box werden (5.00 DM , bzw 2.00 DM / Monat, keine Zeitgebühren)

Ich will Benutzer der INFEX - Box werden (8.00 DM /Monat Mindestnutzung + Zeitgebühr)

(Gewünschtes System markieren, Unterlagen werden zugesandt)

Personenbezogene Daten ab hier eintragen:

Name	
Vorname	
Strasse Hsnr	
PLZ Wohnort	
Elektronische Adresse	

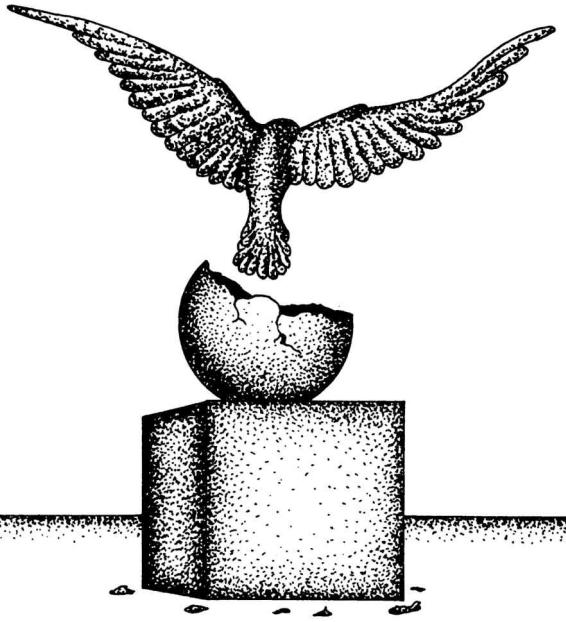
(Angaben auch machen, wenn Adressklebe beigefügt, falls Adressklebe fehlt: 1.00 DM Bussgeld)

Ort,Datum,Unterschrift

Chaos Computer Club e.V. **Schwenckestrasse 85 2000 Hamburg 20**

Kto 59 90 90 - 201 PGirosA Hmb **040 / 490 37 57 GEONET&CLINCH: CHAOS-TEAM**

**Wenn unzustellbar
Anschriftenausschnitt bitte
mit neuer Adresse zurück**



Die Datenschleuder

Aufbruch

R. Schrutki '79.1.1.