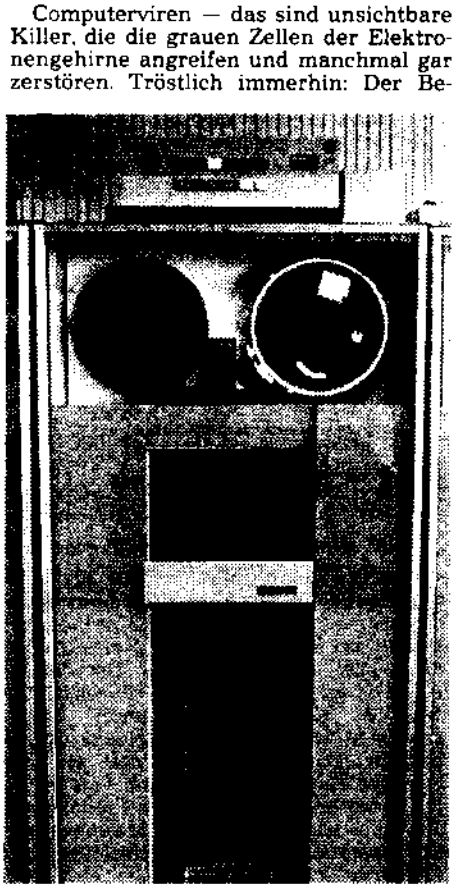
Unsichtbare Killer greifen die grauen

Computerviren schleichen sich in Rechner ein und vernichten Daten / Nur wenige U

Fast kein Unternehmen kann heute auf elektronische Datenverarbeitung verzichten. Immer mehr Arbeitnehmer und Arbeitgeber sind von Tastaturen und Terminals abhängig. In letzter Zeit häufen sich Meldungen über „Viren", die Rechner befallen. Dabei handelt es sich keineswegs um kleine Tierchen. Computerviren sind Programme mit vertrackten Eigenschaften. Sie schleusen sich in fremde Software ein und verändern diese. Und das hat Folgen: Statt normal zu arbeiten, produziert der Rechner weitere elektronische Bazillen. Über infizierte Speicher pflanzt sich

Pop, Push, Add, 0776, 07C4, 0825 — unverständliche und endlos lange Zahlen- und Wort-Kolonnen huschen über den Monitor. Mal tauchen Pfeile, mal Diagramme auf dem gelb-schwarzen Bildschirm auf. „Da erkennt man nicht viel", meint der Heidelberger Physik-Student Bernd Fix. Hinter den Buchstaben, Zahlen und Wörtern verbirgt sich etwas, was Experten als „Büchse der Pandora" oder gar als „Molotowcocktail" des Mikrochip-Zeitalters bezeichnen. Die Codes und Befehlsketten, die Fix auf dem Bildschirm eines Personal Computers vorführt, sind Bestandteile eines Computervirus.

Computerviren — das sind unsichtbare Killer, die die grauen Zellen der Elektronengehirne angreifen und manchmal gar zerstören. Tröstlich immerhin: Der Be-



Magnetbandspeicher: Brutstätte für Viren. Bild: Ungarisch

nutzer braucht keine Angst zu haben, daß winzige Tierchen aus dem Rechner klettern und ihn anstecken. Die „Krankheitserreger" infizieren nur Rechner. Es sind Computerprogramme mit vertrackten Eigenschaften. Sie können lange Zeit schlummern und, plötzlich durch ein Datum oder einen Befehl aktiviert werden.

Einmal munter, schleusen sich die Viren in andere Programmen ein und verändern sie. Die Folge: Wird die infizierte Software benutzt, entstehen neue Viren die weitere, noch nicht verseuchte, Programme befallen. Über verseuchte Disketten — Informationsspeicher, wie sie sich heute in fast jedem Arbeitsplatz- oder Heimcomputer finden — kann sich der Bazillus fortpflanzen, und weitere elektronische Datenverarbeitungsanlagen (EDV) anstecken.

Virus ist nicht gleich Virus. Viele Gattungen und Abwandlungen tummeln sich in der Computerwelt. Experten unterscheiden feinsinnig zwischen Zeit- oder Logikbomben sowie trojanischen Pferden. Die Schäden, die die Eindringlinge anrichten, sind vielfältig. Mal erscheinen auf dem Bildschirm lediglich Jux-Meldungen: „Etwas Wunderbares ist passiert, dein Computer ist lebendig geworden." Oder: „Zimmermann is watching you!" Eher zum Lächeln reizen Warnungen wie „Wassereinbruch im Disketten-Laufwerk", wenn dazu der Lautsprecher das Geräusch von Wassertropfen simuliert.

Außer solch harmlos erscheinenden Späßen richten Viren auch irreparable Schäden an. Dateien können gelöscht, Systemfehler vorgegaukelt, Diskettenlaufwerke beschädigt oder der Rechner so überlastet werden, daß er zusammenbricht. In Computerzentren mehren sich die besorgten Mienen: Wissenschaftler fürchten um Ergebnisse, die sie in langen Jahren zusammengetragen haben. Unternehmen bangen um Kundendateien. Schlimmeres wäre zu befürchten, wenn durch die Killer Roboter in einer Montage verrückt spielen oder elektronische Bankverbindungen zusammenbrechen.

„Die Gefahren von Viren und anderen Manipulationen sind unglaublich. Die Bedrohung ist viel größer als viele Menschen glauben", verrät Donald Latham der New York Times. Latham weiß, wovon er spricht. Er war früher Berater im US-Verteidigungsministeriums und befaßte sich mit der Sicherheit von Computersystemen. Auch beim Bundeskriminalamt (BKA) in Wiesbaden kann man sich vorstellen, daß in Zukunft statt Sprengsätze „Computerviren benutzt werden, um Rechenanlagen lahmzulegen."

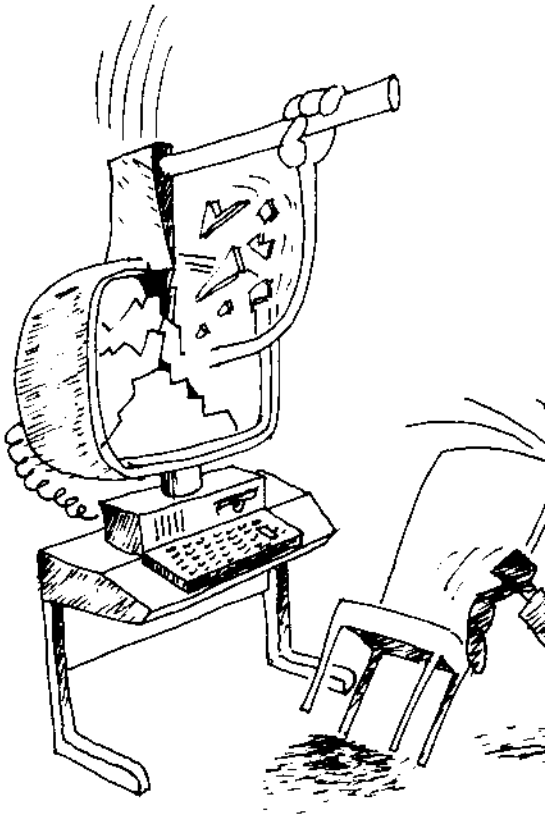
Die Versicherungsbranche ist sich der Risiken ebenfalls bewußt. „Manipulationsverfahren, wie das trojanische Pferd oder der Computervirus stellen eine ernsthafte Gefahr für Datenbestände und Computerkapazität dar", heißt es im letzten Jahrbuch der Assekuranz.

Bislang wurden allerdings nur wenige Fälle bekannt. Was nichts heißt: Viele Firmen wollen einen Vertrauensverlust vermeiden, und halten ihre Schadensmeldungen unter Verschluß. Dem Bundeskriminalamt ist bis heute offiziell kein Fall von Computermißbrauch mittels Virus mitgeteilt worden. Was an die Öffentlichkeit drang, ist aber keineswegs harmlos. Für die meisten Schlagzeilen sorgte der sogenannte „Weihnachtsvirus", der aber streng genommen kein Virus sondern ein elektronischer Kettenbrief war. Erstmals tauchte er an der der Universität Clausthal-Zellerfeld auf und verbreitete sich über das wissenschaftliche Datennetz EARN/BITNET/NORTHNET in kurzer Zeit über die ganze Welt.

Studenten und Wissenschaftler, die ihre Terminals einschalteten, wurde ein kleiner Lustgewinn versprochen. Dazu sollten sie einfach das Wort „Weihnachten" eintippen. Auf der Mattscheibe erschien prompt ein aus Sternchen gebilde-

ter Christbaum garniert mit den besten Wünschen fürs nächste Jahr. Der harmlos anmutende Jux belastete das Rechnernetz enorm: 70 bis 80 Prozent des wissenschaftlichen Datenaustauschs bestand nur noch darin, daß die Fachleute Weihnachtsgrüße hin und her schickten. Anfang des Jahres tauchte dann in den USA eine heimtückische Variante auf. Sie veranlaßt den Benutzer dazu, unbeabsichtigt seine Dateien zu löschen.

Elektronische Bazillen suchten auch die Universität Jerusalem heim. Ein Virus hatte sich in einige Arbeitsplatzcomputer eingeschlichen. Die Folge: Die Anlagen arbeiteten langsamer und am 13. Mai 1988 — so die Drohung — sollten



sich alle gespeicherten Informationen in Luft auflösen. Das konnte zwar noch verhindert werden; aber immerhin pflanzte sich der „Störenfried" fort und richtete im Ausbildungszentrum des israelischen Erziehungsministeriums einen Software-Schaden von 15 000 Dollar an. Ferner verflüchtigten sich die Daten auf zwei Platten — 7000 Arbeitsstunden waren vertan.

Beschäftigten des englischen Verteidigungsministeriums verging ebenfalls das Lachen. Immer wenn sie das Wort Prime Minister oder Margret Thatcher einga-

rauen Zellen der Elektronengehirne an

ur wenige Unternehmen schützen sich vor Millionenschäden durch makabre Scherze

erarbei- ind von Meldun- neswegs kten Ei- rändern er Rech- nzt sich

der Störenfried dann fort. Die Schäden sind vielfältig und kostspielig. Mal erscheinen nur Ulkmeldungen auf der Mattscheibe, mal verschwinden Daten oder das ganze System stürzt ab. Fachleute sehen große Gefahren. Die betroffenen Firmen halten ihre Schäden aus Angst vor Vertrauensverlusten weitgehend unter der Decke. Doch die bislang bekanntgewordenen Fälle stimmen beunruhigend. Einen vollständigen Schutz gegen außer Kontrolle geratene Computerviren gibt es nicht, gewisse Risiken lassen sich jedoch eingrenzen.

en besten er harm- las Rech- zent des uschs be- Fachleute schickten. nn in den ante auf. , unbeab- ten auch n. Ein Vi- platzcom- : Die An- d am 13. — sollten

ben, erschien die eiserne Lady auf dem Bildschirm — stilecht mit Fahne, dem Union Jack. Danach stürzte das System ab. Schließlich mußte ein neues Textverarbeitungsprogramm besorgt werden.

Auf der Insel spielt ein weiterer Fall. Ein elektronischer Krankheitskeim hatte sich ausgerechnet im Computer einer Glasgower Klinik eingenistet. Angeblich wurde die Software der Intensiv-Station beschädigt. Es habe zwar keine Gefahr für Patienten bestanden, betont ein Sprecher der Klinik. Immerhin seien aber wichtige Krankendaten gelöscht worden.

Auch Softwarehäuser haben leidige Erfahrungen mit Viren gemacht. Die amerikanische Aldus Corporation in Seattle

tionen in noch ver- pflanzte richtete elischen Softwa- . Ferner uf zwei n waren

Verteidi- falls das rt Prime r einga-

mußte 5000 Exemplare ihres Software-Pakets zurückrufen. Grund: Der Herausgeber eines Magazines hatte einen Virus eingepflanzt. Anfang März sollte auf den Bildschirmen mancher Rechner eine Friedensbotschaft aufleuchten.

Rolf Hilchner, Chef des Software-Vertreibers **GFA-Systemtechnik in Düsseldorf**, erinnert sich ungern an sein Viren-Erlebnis. Vor kurzem brachte seine Firma ein Buch mit Beispiel-Disketten zu einem neuen Basic-Programm heraus. Etwa 10 000 Speicherplatten waren mit einem Bazillus infiziert. „An einem Wochenende haben wir dann per Hand die verschweißten Bücher aufgerissen und die Disketten ausgetauscht. Da waren noch etwa 8500 Stück auf dem Lager", berichtet er. Wer bereits ein Exemplar gekauft hatte, dem schickte das Unternehmen ein sogenanntes Kill-Programm. Den Schaden beziffert Hilchner auf etwa 20 000 Mark. Woher der Virus stammt, „das wissen wir nicht", verrät der Manager ganz ehrlich. „Der kann über eine verseuchte Kundendiskette oder sonstwie ins System gelangt sein."

Die lästigen Erreger fallen jedoch nicht vom Himmel. Irgendjemand muß sie eingepflanzt haben. Manchmal sind die Urheber Computerfreaks, die ihre Geltungssucht oder ihren Spieltrieb ausleben möchten, glaubt Siegfried Herda, von der Gesellschaft für Mathematik und Datenverarbeitung (GMD): „Die wollen einfach ihre Macht beweisen." Auf der Computerschau Cebit in Hannover bot ein Unternehmen gar einen Virus-Construction-Set an — der Bazillus zum Selberbauen.

Doch nicht nur spielende „Computernarren" treiben Mißbrauch mit dem Rechner. Auch frustrierte Programmierer, die sich von Vorgesetzten schlecht behandelt fühlen, rächen sich mittels Elektronengehirn. Ein britischer Staatsanwalt klagte einen Mitarbeiter an, mit einer „logischen Bombe" Schaden in einer Luftfahrtgesellschaft angerichtet zu haben. Vor Gericht wurde der Vorwurf jedoch fallengelassen.

Andere Computerprofis benutzen Viren als Schutz. Häufig werden nämlich die aufwendig ausgetüftelten Originalprogramme illegal abgekupfert. Um sich vor dem Ideenklau durch Raubkopien zu schützen, pflanzen einige Entwickler eine Bazille bewußt als Wächter in ihr Programm ein — so auch ein pakistanischer Computerfachmann. Immer wenn jemand eine Raubkopie zog, wurde der Krankheitserreger aktiv. Die Folge war das „Pakistanische Fieber", wie das Wirtschaftsmagazin Business Week das Leiden taufte. Außer Kontrolle geratene Mutationen dieses Codes vernichten mittlerweile auf eigene Faust Daten. Inzwischen sind Versionen davon in Israel, Europa und den Vereinigten Staaten aufgetaucht.

Ob nun ein Programmierer sein Geisteskind schützen oder seinen Frust abreagieren will — für den Computerfreak Fix handeln sie alle skrupellos: „Der Schaden, den ein Virus anrichten kann, ist nicht zu überblicken." Er selber würde deshalb nie einen solchen Killer aussetzen. Aus gutem Grund. Seit 1986 ist im Rahmen des 2. Gesetz zur Wirtschaftskriminalität der Computermißbrauch unter Strafe gestellt. Wer Viren pflanzt und erwischt wird, kann danach zu einer Geldstrafe oder Freiheitsentzug bis zu fünf Jahren verurteilt werden.

Der erste, der vor solchen Manipulationen warnte, war 1983 der Amerikaner Fred Cohen, heute Professor an der Universität von Cincinatti. Er wies nach, daß solche Killer innerhalb einer Stunde alle Programme einer Datenverarbeitungsanlage infizieren können. Einzelne seiner Viren schafften es gar in 28 Sekunden.

Cohen wollte mit seinen Experimenten zeigen, wie anfällig Rechenanlagen sind. Gleichzeitig wollte er das Sicherheitsbewußtsein der EDV-Benutzer schärfen. Ob ihm dies gelungen ist, darf bezweifelt werden. In der Bundesrepublik kümmern sich die meisten Firmen, die Computer verwenden, kaum um Sicherheitsfragen, meint Klaus Brunnstein, Informatik-Professor an der Universität Hamburg. Eine Umfrage der Fachzeitschrift Kommunikations- und EDV-Sicherheit unter Banken, Versicherungen, Industrie-Unternehmen und Behörden gibt ihm recht. Danach hat weniger als jede dritte Einrichtung eine ausgeklügelte Strategie um ihre EDV vor Mißbrauch zu schützen.

Ob mit oder ohne Sicherheitsstrategie — gegen Viren gibt es kein Allheilmittel. Da sind sich Siegfried Herda von der GMD und Computerfreak Bernd Fix einig. Die Risiken lassen sich jedoch verringern. Die meisten elektronischen Bazillen tummeln sich in den Personal Computern, weil diese nicht so geschützt sind wie große Rechensysteme. Anwendern kann man nur empfehlen, Programme unbekannter Herkunft zu meiden. Die Hamburger Hackerzeitschrift Datenschleuder warnt angelehnt an die **AIDS-Vorsorge: „Häufiger Disketten**tausch mit wechselnden Partnern bringt ein hohes Infektionsrisiko." Professor Brunnstein sieht das Risiko ähnlich: „Einen promisken Umgang mit verschiedenen Datenquellen sollte der Benutzer meiden."

ANDREAS HOFFMANN

Speicherinhalte frühzeitig kopieren

Die meisten elektronischen Bazillen tummeln sich in Personalcomputern. Wer Schäden durch Viren-Befall eingrenzen will, sollte frühzeitig Sicherheitskopien von wichtigen Dateien anlegen. Es gibt „Kill-Programme", die eine Software nach enttarnten Störenfrieden durchforsten und diese ausmerzen. Andere Hilfen wiederum prüfen jeden Morgen, ob sich über Nacht in den Speichern etwas geändert hat.

Für Großrechenanlagen existieren weitere Schutzbarrieren — etwa, daß nur mehrere Experten zusammen ein Programm ändern können oder bestimmte Verschlüsselungen eingeführt werden. Darüber hinaus lassen sich Daten auch auf nicht nachträglich manipulierbaren Bildplatten speichern.

Inzwischen wurden auch Konstruktionsprinzipien von Rechnern angepaßt. Soll in das System eingegriffen werden, bedarf es verschiedener Schlüssel — so wie sich mancher Banktresor nur mit mehreren Schlüsseln öffnen läßt. Gleichwohl: Findigen Tüftlern könnte es dennoch gelingen, mit ihren Computer-Bazillen auch diese Hürden zu überspringen. aho