Auf die Knie

Ein Virus wurde in amerikanische Datennetze eingeschleust – der erste schwere Fall einer Computer-Infektion.

Furchtbare Kopfschmerzen hat uns das bereitet", stöhnte Clifford Stoll, Experte für Computer-Sicherheit an der Harvard University. „Es gibt nicht einen einzigen Systemmanager, der sich nicht die Haare rauft."

Das allgemeine Wehklagen der amerikanischen Computer-Fachleute begann um neun Uhr am Mittwochabend letzter Woche. Großrechner an Universitäten wie Harvard, MIT und Stanford, aber auch in einer Kommandozentrale der US-Marine in San Diego brachen plötzlich unter der Last von zusätzlicher Rechenarbeit zusammen, die sich zunächst niemand erklären konnte.

Rechner in Flugüberwachungs-Zentrale: „Das ist erst der Anfang"

Doch bald war den Experten klar: Ein sich mit unheimlicher Geschwindigkeit ausbreitendes Computer-Virus war in Netze eingedrungen, die mehr als 50 000 Computer in amerikanischen Militärdienststellen, Forschungseinrichtungen und Großunternehmen verbinden, hatte sich dort immer aufs neue vermehrt und damit gleichsam die Verdauungskapazität der Rechner überfordert.

Am Donnerstag nachmittag letzter Woche bestand für die Sicherheitsexperten der betroffenen Systeme kein Zweifel mehr: Es war die bisher größte Attakke eines Computer-Virus in den USA. Chuck Cole, stellvertretender Computer-Sicherheitsmanager im Lawrence Livermore Laboratory, wo Amerikas Atom- und SDI-Waffen entwickelt werden, formulierte das Entsetzen der Kollegen: „Das Besondere daran ist, daß ein relativ harmloses Virus-Programm buchstäblich unsere gesamte Computer-Gemeinde in die Knie zwingen und eine Weile auf der Matte halten kann." Und er fügte hinzu: „Die Kosten, das angerichtete Unheil wieder auszubügeln, werden enorm sein."

Wer das unheilvolle Virus in die Computernetze eingeschleust hatte, blieb bis Ende letzter Woche rätselhaft. Allerdings meldete sich ein Anonymus telephonisch in der Redaktion der „New York Times" und erklärte: Ein ihm befreundeter Informatik-Student habe im Zuge eines Experiments versucht, ein ihm harmlos erscheinendes Virus in eines der Datennetze einzupflanzen. Dabei sei etwas schiefgegangen, ein winziger Fehler im Programm habe dazu geführt, daß sich das Virus unendlich viel schneller als erwartet dupliziert habe.

Unmittelbar nach dem Starten des Programms habe der Student den Fehler bemerkt und sei nun über die Konsequenzen zutiefst erschrocken. Ein Sprecher des Pentagon, das nach Bekanntwerden der Virus-Malaise einen Krisenstab einrichtete, hielt die Version des anonymen Anrufers für „plausibel".

Demnach wäre in den Computer-Netzen nun zum ersten Mal passiert, was die Kritiker der Gentechnik auf ihrem Gebiet immer befürchten: daß sich ein Krankheitskeim selbständig macht und ein unvorhersehbares Übel verbreitet. Der Begriff Computer-Virus folgt dem biologischen Modell: Es ist ein Programm oder eine Kette von Befehlen, die – wie das Virus in der menschlichen Zelle – den Wirtscomputer zwingen, nach ihrem Kommando zu operieren, womöglich lange Zeit als „schlafende Viren", von niemandem bemerkt.

Schon seit 1983 haben Computer-Fachleute über das Problem von Computer-Viren in Expertenzirkeln diskutiert. Seit Beginn des Jahres 1987 wurden erste Fälle von Virus-Ausbreitung gemeldet. Doch bislang waren meist nur vergleichsweise kleine Anlagen betroffen, auf der Ebene von Personal-Computern.

Kopierte Software für PCs etwa der Hersteller IBM, Apple und Commodore kam gelegentlich mit milden Virus-Infektionen auf den Markt – mit dem Effekt, daß Text- oder Graphiksysteme am Bildschirm zusammenbrachen.

Auch größere Netze waren schon befallen, zum Beispiel als im Dezember 1987 ein deutscher Student aus Clausthal-Zellerfeld eine Weihnachtsbotschaft ins IBM-Netz einschleuste: Auf den Schirmen erschien ein stilisierter Weihnachtsbaum. Die in geometrischer Progression ansteigende Vervielfältigung der Nadelbaum-Graphik zwang den Konzern, sein „Bitnet" in Europa und den USA stillzulegen, bis der elektronische Weihnachtsgruß eliminiert war.

Tagelang litt eine Zeitungsredaktion in Providence (US-Staat Rhode Island) unter einem Virus, das über einen der PCs ihrer journalistischen Mitarbeiter eingeschleust worden war. Das „Journal-Bulletin" kam ohne nennenswerten Schaden davon, lediglich einer Reporterin wurden alle elektronisch gespeicherten Manuskripte und Notizen gelöscht. Schlimmer waren die Folgen einer Virus-Infektion für ein Krankenhaus-Zentrum an der amerikanischen Ostküste: Dort wurden, im Herbst 1987, 40 Prozent der Patientenkartei vernichtet.

„Aber das ist erst der Anfang", sagt Harold Highland von der Zeitschrift „Computers & Security", der sich seit Jahren mit Computer-Viren befaßt. Die Experten für Computersicherheit bei amerikanischen Banken zittern vor einem denkbaren Desaster: So abhängig sind sie vom einwandfreien Funktionieren der inzwischen weltweit vernetzten Kommunikationssysteme, durch die Milliardenbeträge hin- und hergebucht werden, daß ein bösartiges Virus katastrophale Folgen haben müßte.

Nicht minder verletzbar sind andere hochsensible Rechnernetze: in der Versicherungsbranche etwa, bei der Flugüberwachung, bei der Verbindung zwischen internationalen Börsenplätzen, aber auch bei der Lenkung der Verkehrsströme in den Metropolen.

„Das Unglück mußte geschehen, wir haben es nicht anders verdient", klagte Geoffrey Goodfellow von der Anterior Technology Inc. über die Virusinfektion, die sich in der letzten Woche ereignet hat. „So etwas mußte passieren, damit wir zu Verstand kommen." Bisher seien in Computer-Netzwerken zu wenige Vorkehrungen gegen Virus-Angriffe getroffen worden.

In Windeseile ausgebreitet hatte sich der Stör-Keim in dem Forschungszen-

tren-Verbundnetz „Internet" sowie in den Computernetzen „Arpanet" und „Milnet", die dem Informations- und Datenaustausch vor allem zwischen Universitäten und Auftragnehmern des Pentagon dienen. Über Arpanet, das 1969 installiert wurde, laufen zum Beispiel Projekt-Informationen, Kostenrechnungen und Forschungsresultate – Daten, die keinem speziellen Geheimnisschutz unterliegen. Da besonders benutzerfreundlich, galt Arpanet den Experten von jeher als anfällig für Eindringlinge.

Deshalb wurde 1983 „Milnet" davon abgespalten, als Netz für den Austausch militärischer Daten von höherem Sicherheitsrang; Daten der höchsten Geheimhaltungsstufe, etwa über den Einsatz von Atomwaffen, werden auf diesem Netz jedoch nicht ausgetauscht.

Am Freitag letzter Woche waren Computer-Experten so weit, daß sie das eingedrungene Virus-Programm analysieren konnten. Ergebnis: Das Programm sei „mit bemerkenswertem Geschick" geschrieben. Es enthüllte drei Sicherheitslücken im Arpanet-System, über die es eingeschleust worden war. Ein Teil des Programms diente dazu, Zugangscodes zu Rechnern ausfindig zu machen; so als „berechtigter Benutzer" ausgewiesen, konnte das Virus in die Rechner eindringen und sich dort tausendfach von Maschine zu Maschine vermehren.

Zahlreiche Teilnehmer, vor allem Militärs und militärische Forschungsinstitute wie Lawrence Livermore, kappten ihre Verbindungen zum Verbundnetz, um ihre Rechner und Programme vom Virus zu befreien. „Das Virus zu killen", umschrieb Paul Pomes von der University of Illinois in Urbana-Champaign die elektronische Kammerjägerei, sei „einfach" – das Unterfangen aber, „auch alle Töchter-Viren zu erwischen", eine „harte und trickreiche Aufgabe".

Bisher waren alle Versuche von Computer-Wissenschaftlern, die Rechner mit geeigneten Abwehr-Programmen, also gleichsam einer Immunabwehr gegen Viren, auszustatten, wenig erfolgreich. Impfprogramme gegen Computer-Viren bieten nur begrenzten Schutz. Die einzige Möglichkeit, hochgefährdete, etwa militärische Systeme gegen Eindringlinge abzuschirmen, bleibt die Isolierung der Rechnersysteme gegenüber der Außenwelt. Schutz vor Sabotage im Innern bietet auch das nicht.

Andererseits könnten die Viren, heute noch relativ harmlos, immer subtiler und gefährlicher werden. Computer-Wissenschaftler wie Ian Witten von der University of Calgary in Kanada rechnen fest mit der Möglichkeit, daß besonders tükkische Viren („Monster"-Programme) in die Betriebssysteme von Großrechnern gepflanzt werden und jahre- oder jahrzehntelang unentdeckt bleiben könnten. Wenn sie dann auftauchen und ihr Verwirr- oder Zerstörspiel beginnen, hätte man kaum mehr die Möglichkeit, sie auszuschalten. ◆