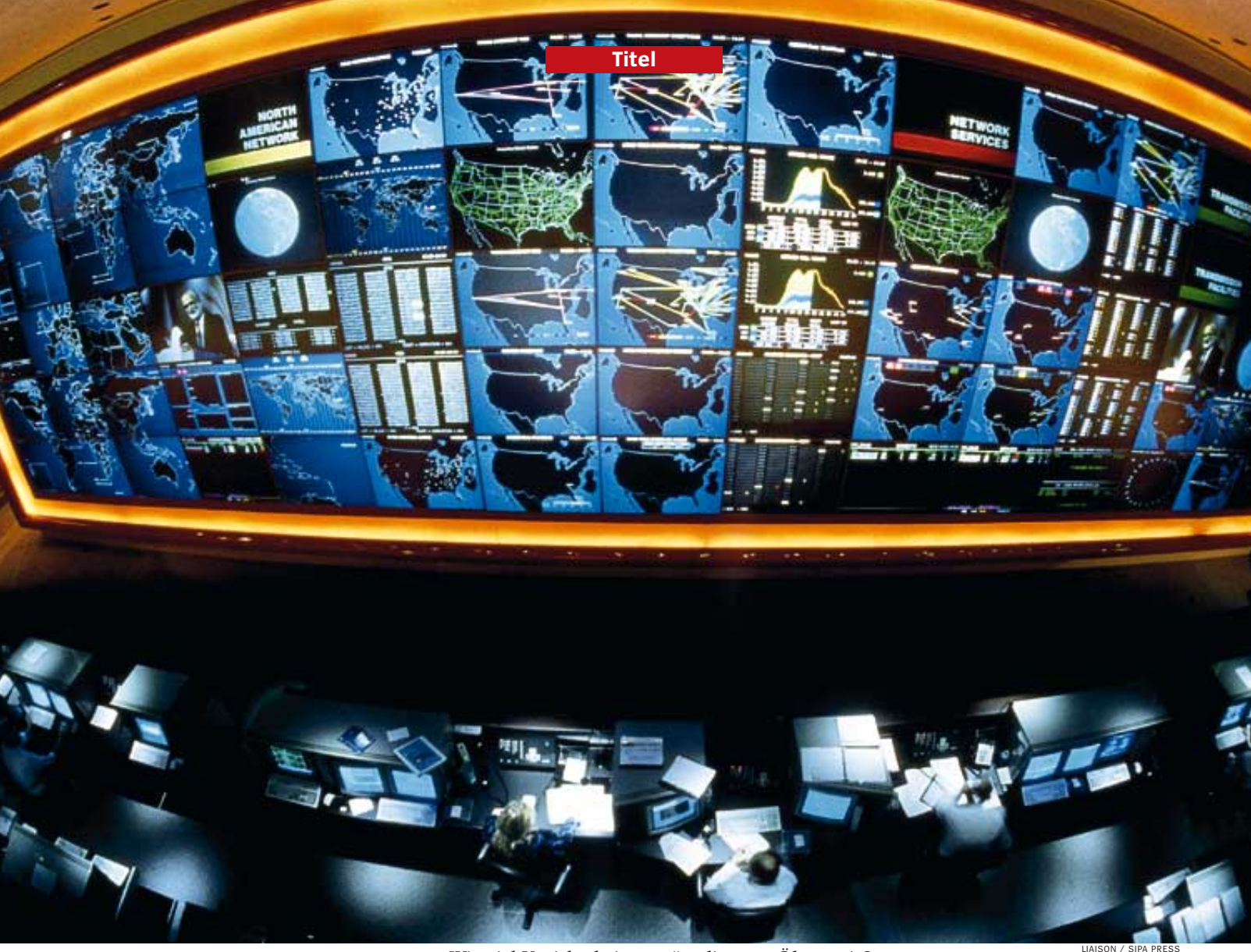


Schaltzentrale des US-Telefonkonzerns AT&T: *Wie viel Unsicherheit verträgt die neue Ökonomie?*

LIAISON / SIPA PRESS

@ttentäter im Netz

Internet-Piraten halten die Welt in Atem: Mit Viren zerstören sie Daten von Firmen, via E-Mail legen sie Kommunikationsnetze lahm, mit Hackermethoden spionieren sie die Privatsphäre von Bürgern aus. Ihre einzige Konkurrenz sind Geheimdienste und Militärs – auch sie operieren per Internet.

Ihre Symbole sind düster. Sie sind der Drogenwelt entliehen, den Vernichtungsspielen für Computer oder dem Suicide-Rock der Gruppe Nirvana: Giftzeichen, Totenköpfe und Blutspritzer.

Ihre Namen sind verschlüsselt, sie nennen sich „The Analyzer“, „Sir Dystic“ oder „Dark Angel“. Ihr Instrumentarium könnte einem Fantasy-Roman entstammen. Sie setzen ansteckende Viren frei oder monströse Würmer, kommandieren Dämonen oder Trojanische Pferde. Ihre weltweiten Angriffe kommen aus dem Hinterhalt, haben die Wucht von Bomberladungen und sind für die Opfer verheerend.

Noch bis vor kurzem war die Welt der Computerhacker für die meisten eine abstruse Spielecke kontaktgestörter Kids mit dicken Brillengläsern. Doch spätestens seit dem Angriff mit dem Virus „I love you“ haben die Keyboard-Freaks ihre Unschuld verloren. Die Zwischenfälle mussten auch dem letzten Technologie-Begeisterten klarmachen, dass die neue Computerwirtschaft nicht nur aus Gründerstars, genialen Tüftlern und ihren Erfolgsgeschichten besteht. Der schönen neuen Online-Welt folgt ein Schatten, dessen Umrisse ebenso rasch wachsen wie das globale Computernetz: eine Unterwelt aus jugendlichen Vandalen, Kriminellen und den ersten Cyber-Terroristen.

Was die Online-Welt an neuen Möglichkeiten beinhaltet – Innovation, Selbstverwirklichung, Spaß, Reichtum –, bietet sie zwangsläufig auch an Zerstörungskraft. Schon heute ist das Internet eine eigene Welt mit einer eigenen Wirtschaft, eigenen Gesetzen und eigenem Geld. Nun wird klar, dass es auch seine eigene Form von Verbrechen, Sabotage und sogar Krieg hervorbringt.

Im Untergrund der Computerszene, in Studentenzimmern, Garagen oder abgelegenen Fabriketagen hat sich ein Potenzial

D. SMITH / BLACK STAR

Hackergruppe LOpht (in Boston): *Angriffe aus dem Hinterhalt*

Computerviren

PHANTOM Infiziert Dateien mit sinnlosem Datenschrott

ANXIETY Verwandelt den Mauszeiger in eine Spritze, bis schließlich der Rechner abstürzt

aus Saboteuren zusammengefunden, das die Sicherheit von Staaten und das reibungslose Funktionieren der Wirtschaft bedroht. Ein Aldi-PC genügt, um von Köln-Porz oder Pinneberg aus nicht nur die Online-Welt aus den Angeln zu heben.

Das Internet ist eine irreale Gratis-Spielwiese geworden, das Netz kostet kaum Geld und bietet die Möglichkeit, den Erwachsenen schnell und brutal zu zeigen, wer man ist – und *dass* man ist. Ich zerstöre, also bin ich.

Betroffen vom Größenwahn und den Allmachtsphantasien einer Horde von Hackern sind inzwischen Menschen auf der ganzen Welt. Rund 304 Millionen nutzen heute in Firmen, Behörden oder zu Hause das World Wide Web und jagen täglich Milliarden E-Mails durch das Datennetz. Konzerne tauschen Firmengeheimnisse aus, Krankenkassen die Malaisen ihrer Kunden, Behörden vertrauliche Gesetzesvorlagen, Bürger ihre Geldgeschäfte – oder intimste Liebesaffären.

Doch je mehr Daten über das Weltnetz zugänglich sind, umso größer sind die Chancen für die neue Unterwelt, sie anzuzapfen, zu manipulieren oder zu zerstören.

Computerkriminelle dringen in die Kundendateien von Online-Einkaufszentren, erobern die Rechner von Banken, Behörden, sogar Regierungen. Im März verhafteten britische Ermittler zwei walisische Teens, die sich unter dem Pseudonym „Curador“ 26 000 Kreditkartennummern aus den Computern von Online-Kaufhäusern kopiert hatten – darunter auch die von Microsoft-Gründer Bill Gates.

Sicherheitsexperten wie der Siemens-Manager Hermann Kampffmeyer fürchten gar, das globale Elektroniknetz könnte schon bald zum Tummelplatz für eine neue Generation von Terroristen werden, die, anders als die RAF, zwar nicht prominente Wirtschaftsführer, dafür aber den kompletten Datenbestand von Großunternehmen ver-

„Ein stiller Schüler“

Ein Streich oder die Rache für eine abgelehnte Examensarbeit? Zwei Informatikstudenten aus Manilas Vororten haben offenbar das Computervirus „I love you“ freigesetzt.

Wer in Manilas Stadtteil Pandacan lebt, gehört nicht zu den Ärmsten unter den Bewohnern der philippinischen Hauptstadt. Die schäbigen Betonhäuser entlang der mit Schlaglöchern übersäten Zamora-Straße gelten nach Definition der Einheimischen des hässlichen Zehn-Millionen-Molochs als passables Wohnquartier.

„Wir sind ganz einfache Leute hier, die für wenig Geld hart arbeiten“, sagt Irene de Guzman, 26, ein schüchternes Mädchen mit Pickelgesicht. „Wir tun niemand etwas zu Leide und haben ansonsten auch nichts Böses im Sinn.“

Die jungen, drahtigen Agenten des National Bureau of Investigation (NBI), der philippinischen Ausgabe des FBI, haben da ihre Zweifel. Am Montag Nachmittag stürmten acht Agenten der Abteilung für Computerverbrechen und Betrug, unterstützt von zwei FBI-Computerfachleuten, die Erdgeschosswohnung der Bankangestellten de Guzman.

„Verdacht auf schweren Betrug und Computerkriminalität“ stand auf dem Hausdurchsuchungsbefehl. Von ihrer Telefonnummer 592-0683 in Manila, so hatte der philippinische E-Mail-Betreiber Sky Internet der Polizei gesteckt, sei das so genannte Love-Virus abgeschickt worden. Jene Computerplage, die in der Vorwoche weltweit Rechner zum Absturz brachte und eine Schadenssumme von geschätzten 20 Milliarden Mark zurückließ.

Was jedoch zu Wochenbeginn in Manila noch wie ein spektakulärer Fahndungserfolg kluger Cyber-Polizisten aussah, entwickelte sich in den Tagen nach der Durchsuchung zur blamablen Posse. Zwar gelang es den Beamten, die 80 Quadratmeter große Wohnung innerhalb kurzer Zeit in ein Schlachtfeld zu verwandeln – nur ein buntes Stickbild („Das letzte Abendmahl“) und das Foto-Antlitz von Papst Johannes Paul II. fielen nicht von der Wand.

Doch noch nicht mal den Computer, den Nachbarn stets hinter dem Vorhang hatten flimmern sehen, konnten die Fahnder auftreiben. „Es müssen wichtige Unterlagen beiseite geschafft worden sein“, erkannte der Leiter der Einsatztruppe, Elfren Minesos.

Außer 17 Computerdisketten, einem Leitfaden „Einführung Windows 95“ und sechs Telefonapparaten nahmen die Beamten nach zweistündiger Durchsuchung gleich noch Reonel Ramones, 28, mit. Der Lebensgefährte von Irene de Guzman war eher zufällig in das von der Polizei inszenierte Chaos gestolpert.

„Der Mann ist der Hauptverdächtige“, tönte Computerkommissar Minesos bald und ließ ihn mitnehmen. Doch auch das war eine Fehlanzeige: Nach 18 Stunden war Ramones wieder frei. Denn es gibt kein Gesetz auf den Philippinen, das den Hackern ihr Handwerk verbietet. Auch konnte der Kassierer einer lokalen Bank glaubhaft versichern, dass er sich nicht mit Computern auskenne und das Internet für eine „langweilige Sache“ halte.

Zum Glück wohnen in Asien ja immer gleich ganze Familienclans eng zusammen. Schnell lenkten die hilfreichen FBI-Agenten das Interesse ihrer NBI-Kollegen auf Onel de Guzman, 23. Der kleine, schüchterne Bruder von Irene, der ebenfalls in der Wohnung gemeldet ist, hört nicht nur Punk-Musik, sondern studiert auch am AMA-Computer-College. In der Privatschule werden 15 000 junge Leute zu Program-

S. BALATAN / ASIA PIX

DPA

Computervirus
Trojanisches Pferd

S. BALATAN / ASIA PIX

Student de Guzman, Internet-Café*
„Das ist illegal“

* Oben: mit Schwester Irene de Guzman; unten: in Manila.

mierern ausgebildet. Schon hatte die philippinische Presse eine „Abu Sayyaf“ des Cyberspace gewittert.

„Nicht ganz zu Unrecht“, offenbarte der Schulleiter Russel Diona tags darauf. Gerade am 24. Februar habe Onel (ein „stiller Schüler“) eine Examensarbeit mit kompromittierendem Inhalt eingereicht. Unter dem Titel „Trojanisches Pferd zur Passwortsuche“ habe sich die Studie damit beschäftigt, „wie man am besten Passwörter stiehlt“. Detailliert beschrieb er darin, wie man in das Adressenverzeichnis eines „gegnerischen“ Computers eindringen könne, wie es das „I love you“-Virus gut zwei Monate später tat.

Als der Schulleiter daraufhin entrüstet auf die Arbeit schrieb: „Das ist illegal“ und „Wir bilden keine Einbrecher aus“, kam es zum Eklat. Der stille Junge verließ das Büro des Dozenten mit den Worten: „Okay, das ist Ihre Entscheidung.“

Und noch eines wusste der Schulleiter zu berichten. Ausdrücklich habe sich der Student Michael Buen, ein Lehrgangskollege von de Guzman, in seiner Abschlussarbeit lobend über den „hilfreichen Freund“ ausgelassen. Buen hatte ein Programm entwickelt, das binnen Sekunden Computerverzeichnisse vernichtet. „Das bedeutet nicht, dass sie gemeinsam das Liebes-Virus geschrieben haben“, sagt Schulleiter Diona, „wir schließen es aber nicht mehr aus.“

„Mein Sohn ist kein Computerkrimineller“, wehrt Mutter Emma de Guzman, 49, ab. „Alles ist ein fürchterliches Missverständnis.“ Mit dem Verkauf von Tupperwaren habe sie sein Studium finanziert. Stolz führt die Frau Neugierige vor den veralteten Computer mit einem 586er Prozessor, der im engen Schlafzimmer ihrer Wohnung in Manilas Stadtteil Makati neben Stockbetten für die jüngeren Geschwister steht. „Einen Internet-Anschluss kann sich mein Sohn gar nicht leisten“, sagt die Mutter. „Der verschlingt so viel, wie ich in der Woche verdiene.“

Und das sei eben ungerecht, verkündet Onel de Guzman einen Tag später vor der Presse. Nachdem der junge Hacker sich 24 Stunden lang mit Schwester Irene vor der Polizei versteckt hatte, sprach er am Donnerstag mit Anwalt Rolando Quimbo zu Journalisten. „Das Internet ist doch zur Ausbildung da, und das sollte sich auch jeder in der Dritten Welt leisten können“, fand der Hacker, meist stammelnd und von Heulkrämpfen unterbrochen. Ob das ein Eingeständnis sei, dass er das Virus in Umlauf gesetzt habe?

„Nein“, sagt de Guzman, „aber vielleicht habe ich ja mal auf den falschen Knopf gedrückt und das Ding losgeschickt.“ Dann schießt ihm wieder Wasser in die Augen. JÜRGEN KREMB

AP

US-Präsident Clinton: *Es gibt kein geschütztes Staatsgebiet mehr*

nichten wollen. „Derzeit turnen im Internet nur Laien rum“, warnt er, „wenn echte Profis das Medium entdecken, dann Gnade uns Gott.“

Wozu Saboteure in den sechziger und siebziger Jahren noch Sprengstoff und Brandsätze benötigten, dafür reicht heute ein Computer und ein Modem. Und wo Staaten früher noch Bomber und Kanonen brauchten, genügt ihnen heute ein simples Rechenzentrum. „Wir haben die besten Hacker der Welt“, rühmte sich Ende vergangenen Jahres der russische Politiker Wladimir Schirinowski und kündigte an, seine ausländischen Feinde künftig mit Computerviren zu attackieren.

PRETTYPARK
Späht Nutzerdaten aus, versendet sie in Chat-Kanäle, ermöglicht Fernsteuerung

Schon warnen Regierungskommissionen in den USA und Deutschland vor einem neuen Cyberkrieg. Es gebe „kein geschütztes Staatsgebiet mehr, das an seinen Grenzen mit militärischen Mitteln zu verteidigen wäre“, hält die geheim tagende Regierungsarbeitsgruppe „Informationstechnische Bedrohung für Kritische Infrastrukturen“ (Kritis) fest. Eine „grundsätzlich neue Situation der Unsicherheit“ sei eingetreten.

Monokultur Microsoft

Lange Zeit hielten Bürger, Politiker und Manager solche Mahnungen für überzogen. Immer wieder hatten sich düstere Zukunftsvisionen als groteske Übertreibungen herausgestellt. Weder hatte sich die Gesellschaft in eine Techno-Diktatur verwandelt, wie es der Literat George Orwell in seinem Werk „1984“ beschrieben hatte, noch hatten sich die Warnungen der Jahr-2000-Skeptiker vor einem globalen Computercrash zum Neujahrstag bewahrheitet.

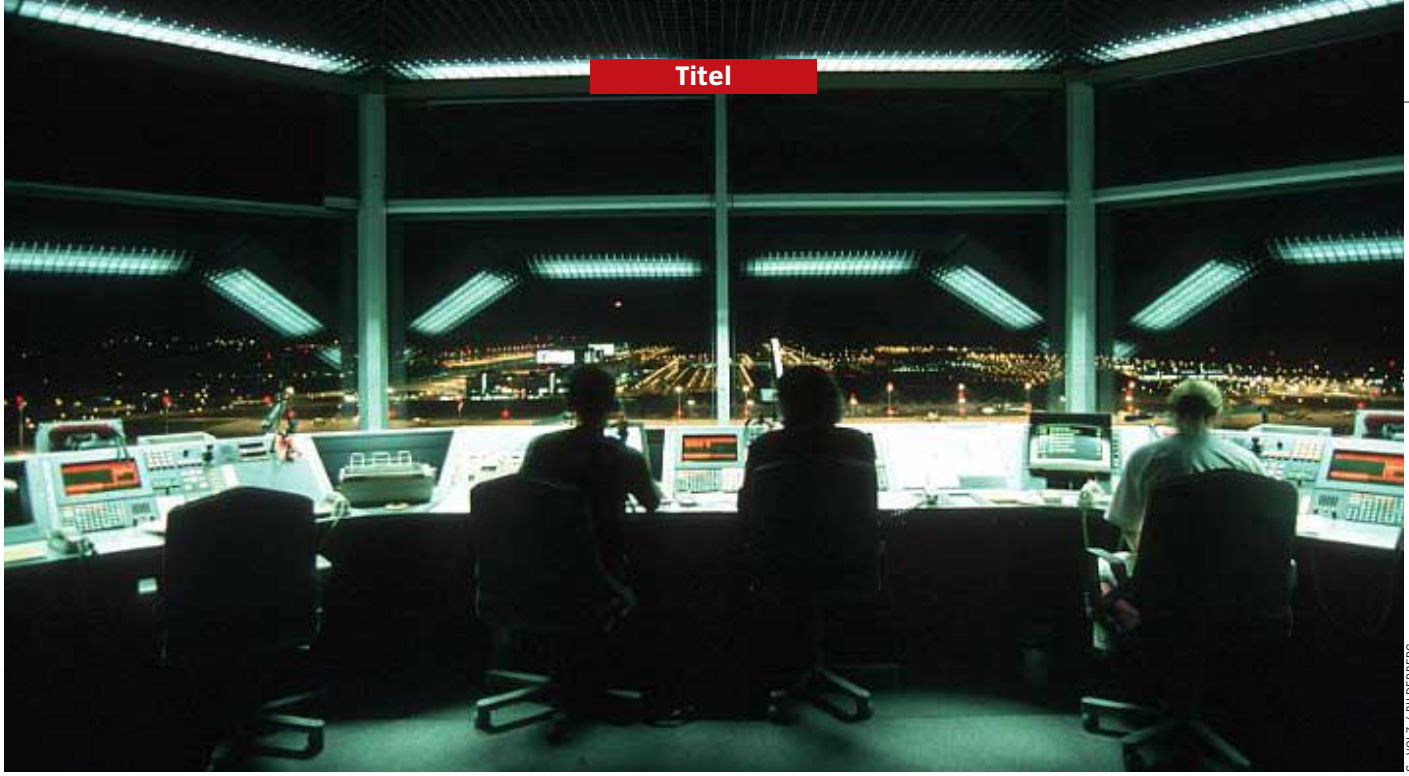
Doch nun offenbaren sich Risiken, die für die Zukunft der Weltökonomie weitaus bedrohlicher sind als die Schattenentwürfe der Technologie-Skeptiker. Die neue dynamische Hightech-Ökonomie mit ihren machtvollen Rechenzentren, Robotern und Digitalarchiven ist so leicht aus der Bahn zu werfen wie die Mercedes-A-Klasse.

Staunend registrieren die Menschen, wie ein winziges Virus die ganze Welt in eine weltweite Computerkrise stürzen kann. Und die war nicht von machtvollen Großrechnern lanciert worden, sondern von einem handelsüblichen PC auf dem heimischen Schreibtisch.

Das von dem philippinischen Studenten Onel de Guzman programmierte Teufelsding, das sich Anfang Mai mit der Botschaft „I love you“ in den Mailboxen der Empfänger ankündigte, lähmte viele Konzerne der westlichen Welt, brachte Millionen Menschen an ihren PC zur Verzweiflung und trieb Regierungen zu Krisensitzungen zusammen. Wie ein asiatisches Grippevirus sprang das angeblich „versehentlich“ freigesetzte Programm mit rasender Geschwindigkeit von Metropole zu Metropole.

In Deutschland erschienen Zeitungen wie die „Mittelbayerische Zeitung“ als Notausgabe, in Belgien legte das Virus die Bargeldautomaten lahm. Es blockierte Rechnersysteme von Konzernen wie Ford und Siemens und infizierte 80 Prozent der amerikanischen Regierungsbehörden – einschließlich des Außenministeriums und des Pentagon. Weltweiter Schaden durch Arbeitsausfall und Reparaturmaßnahmen: rund 20 Milliarden Mark.

Erleichtert wird den Saboteuren das Geschäft durch die Besonderheiten der Mausklick-Ökonomie. Rund 264 Millionen Menschen auf der ganzen Welt nutzen heute das Betriebssystem „Windows“ des Software-Konzerns Microsoft. Das ist praktisch, weil sich Daten unkompliziert hin



S. VOLZ / BILDERBERG

Leitstelle am Flughafen München: *Sabotage via Mausklick?*

und her schicken lassen und Freunde oder Kollegen sich rasch helfen können.

Auf der anderen Seite macht die globale Monokultur das System anfällig. Ähnlich wie Schädlinge sich auf den schier endlosen Äckern der modernen Farmen viel rascher ausbreiten können, pflanzen sich auch Viren und digitale Würmer im globalen Microsoft-Reich mit zerstörerischer Gewalt und Geschwindigkeit fort.

Bundesinnenminister Otto Schily will deshalb nach den Erfahrungen mit dem Liebes-Virus die Behörden dazu anhalten, vermehrt Produkte von Microsoft-Rivalen zu nutzen. „Ich bin dafür, dass wir eine Vielfalt von Systemen einführen“, sagte der SPD-Politiker vergangene Woche und plädierte vor allem für das Microsoft-Konkurrenzprodukt Linux.

Zudem zeigte sich immer wieder, dass die Sicherheit beim Konkurrenzkampf der Software-Konzerne und Online-Firmen nicht gerade Priorität hat. So werden Programme und Computer so schnell weiterentwickelt, dass Schutzmaßnahmen schnell veraltet sind.

Außerdem bringen Software-Firmen, gedrängt von der eigenen Marketingabteilung und ungeduldigen Aktionären, immer wieder Programme auf den Markt, die noch nicht ausgereift sind. Deren Fehler und Lücken bieten Hackern und Vandalen willkommene Angriffsziele und verursachen immer wieder Pannen. Doch nun stellt sich die Frage: Wie viel Unsicherheit verträgt die neue Ökonomie?

Noch nie war es möglich, mit einem so geringen Aufwand weltweit einen derart gewaltigen Schaden anzurichten. Auf rund 2000 Websites finden Cyber-Piraten Munition für ihr digitales Arsenal: elektronische Viren, Würmer, Bomben und andere Zerstörungsprogramme. Sekundenschnell und immer umsonst. Und täglich kommen neue Sabotageprogramme hinzu.

Auch für Gauner und Spione steht längst eine ansehnliche Auswahl im Netz bereit. Kreditkartengeneratoren filtern Nummern aus dem Cyberspace, Passwortknacker wie das vom Profi-Hacker „Mudge“ entwickelte „LOphtcrack“ helfen dabei, das richtige Passwort oder die benötigte Geheimzahl herauszufinden. Anders als am Geldautomaten, wo die ec-Karte nach drei Fehlversuchen eingezogen wird, kann der Hacker in aller Ruhe zahllose Versuche starten.

Verheerende Viren, ähnlich wie „I love you“, lassen sich bereits von Laien im Lego-Prinzip zusammenklicken. Auf etlichen Websites werden inzwischen mehr als 60 Bausätze angeboten – oft versehen mit dem Hinweis: „nur zu Lehr- und Testzwecken“.

„Mit diesen Werkzeugen können Sie völlig ohne Programmierkenntnisse inner-

FOTOS: AP (li. u. M.)

Hacker Kevin Mitnick, Ehud Tenebaum

Hackersoftware „Back Orifice 2000“

H.-G. OED

Minister Schily: *Taskforce gegen Cyber-Terror*

halb weniger Minuten Ihren eigenen Virus im Handumdrehen produzieren“, wirbt etwa ein deutscher Internet-Anbieter. „Sie können den Viren natürlich auch einen Namen geben oder z. B. einstellen, dass der Virus sich an Ihrem Geburtstag aktiviert“, heißt es.

Das Prinzip der digitalen Plagegeister, die immer mehr Computer befallen, ist einfach. Es sind getarnte Programme, die den Computer heute meist per E-Mail erreichen. Neben dem normalen Text enthält der elektronische Brief einen Anhang, der per Doppelklick aktiviert wird. Sekunden später beginnt das Virus, ohne dass der User es merkt, sein Zerstörungswerk. Für ihn sichtbar öffnet sich meist nur ein neues Fenster mit einer Botschaft, einem Foto oder einem Musikstück. Im Hintergrund jedoch greift das Virus auf das Betriebssystem zu: Es vernichtet oder verändert Dateien, beeinträchtigt die Funktion von Programmen oder installiert eine Software, mit der zum Beispiel die Festplatte des Opfers ausgespäht werden kann.

AP (li.)

Zugleich sorgt das Virus oft für seine eigenen Nachkommen, indem es sich automatisch auf jede in den Computer gesteckte Diskette kopiert. Wird die Diskette auf einem anderen PC benutzt, entfaltet das Biest auch dort seine Leistung.

Beim Liebesbrief aus Manila zum Beispiel griff das Virus zunächst auf die Adressenkartei des Mailsystems „Outlook“ von Microsoft. An alle dort verzeichneten Namen schickte es automatisch eine Kopie des heimtückischen Liebesbriefs und sorgte so für eine schlagartige Verbreitung.

Durch die weltweite Kettenbriefaktion wurde zwar das elektronische Postsystem stark beeinträchtigt, weil die Mailstationen die Masse der Nachrichten nicht mehr bewältigen konnten. Schaden im Computer entstand dadurch aber noch nicht.

Den produzierte das Virus erst im zweiten Arbeitsgang. Es durchsuchte heimlich die Festplatte und löschte und veränderte Dateien mit bestimmten Endungen. Digitale Bilder wurden unwiderruflich gelöscht, Musikdateien des Typs MP3 wurden umbenannt und für den Anwender versteckt.

Im dritten Arbeitsgang wies der Eindringling den Internet-Explorer an, bei einer Web-Seite auf den Philippinen eine bestimmte Spionagesoftware abzurufen. Dieses Programm wurde allerdings bei den meisten vom Love-Bug befallenen Computern nicht mehr ausgeführt, da der Server in Asien schnell abgeschaltet wurde. Wäre das Programm aktiviert worden, dann hätte es alle auf der Festplatte gespeicherten Passwörter gesammelt und heimlich als E-Mail auf die Mailbox des Virenschöpfers geschickt.

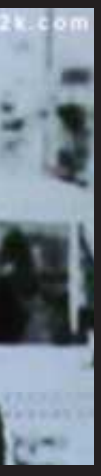
Wie groß das Ausmaß der Computerangriffe schon ist, lässt sich kaum ermitteln. Sicher ist, dass mittlerweile selbst Regierungen und Konzerne Hackertaktiken nutzen, um ihre Gegner zu sabotieren oder Geheimnisse auszuspionieren. „Hacking ist heute eine der drei wichtigsten Methoden, um an Handelsgeheimnisse heranzukommen“, sagt Richard Power vom Computer Security Institute in San Francisco.

William Malik, Computeranalyst der amerikanischen Gartner Group, berichtet von einem Fall, bei dem zwei Konzerne um einen 900-Millionen-Dollar-Auftrag rangen. Spezialisten der einen Firma hackten sich während der Verhandlungen in die Rechner der Konkurrenz und besorgten sich dort E-Mails der leitenden Manager. Prompt unterboten sie das Unternehmen und gewannen den Kontrakt.

Die Virenjäger

Nur in wenigen Fällen fliegen derartige Einbrüche auf. Bei einem heimlichen Testangriff, den die amerikanische Defense Information Systems Agency auf ihre eigenen Rechner in Gang bringen ließ, merkten nur vier Prozent der Computerverantwortlichen in der Agentur, dass Außenstehende in die Systeme eindrangen. Von diesen meldeten weniger als ein Prozent den Zwischenfall an einen Vorgesetzten, obwohl die Angreifer insgesamt 38 000 Attacken ausführten.

Auch Konzerne und Banken scheuen sich, die Hackertaten anzuzeigen, weil sie öffentliche Blamage fürchten. Selbst in der vertraulichen Arbeitsgruppe Aksis, gebil-



Hacker „Mudge“, Web-Seiten für Hacker

PIXEL & ZEICHEN

Hackertreffen „Hope“ (in New York): *Bunter Mutantenzoo*

det von den Sicherheitsmanagern führender deutscher Konzerne, weigern sich die EDV-Experten, offen zu reden. Noch nie, sagt ein Teilnehmer, habe dort eine Firma über Angriffe auf ihre Systeme berichtet.

Doch Zahlen von vertraulich arbeitenden Sicherheitsbehörden und Ermittlern lassen erahnen, dass Computerangriffe mittlerweile so alltäglich sind wie Graffiti in der Berliner U-Bahn. In den Metropolen der Welt, in asiatischen Studentenmansarden, kalifornischen Garagen oder den Hinterhofwohnungen europäischer Metropolen hat sich die Mausklicksabotage zu einer Art Untergrundsport entwickelt, der 1999 allein in den USA Schäden von rund zehn Milliarden Dollar anrichtete.

Das amerikanische Computer Security Institute, das gemeinsam mit dem FBI eine alljährliche Sicherheitsumfrage auswertet, berichtete vergangene Woche, dass 90 Prozent der Konzerne und Behörden, die den Fragebogen zurückgaben, in den vergangenen zwölf Monaten Störungen der Computersicherheit registrierten. 273 Unternehmen und Organisationen oder 42 Prozent der Befragten konnten oder wollten ihre Verluste beziffern: ein Gesamtschaden von insgesamt 265 Millionen Dollar, rund doppelt so viel wie im Durchschnitt der drei Vorjahre.

Längst haben auch die Feinde der Demokratie die zerstörerische Kraft erkannt, die sich mit einem handelsüblichen PC entfalten lässt. „Wir müssen lernen, unsere Feinde mit elektronischen Angriffen zu attackieren“, druckte kürzlich die chinesische Militärzeitung „Jiefangjun Bao“ und rief dazu auf, im Ernstfall den Feind „elektronisch“ in die Knie zu zwingen.

Wie einfach sich das bewerkstelligen lässt, rechnen Experten im amerikanischen Pentagon vor. Statt einer hoch gerüsteten Armee reichten heute 30 Computervirtuosen, um die Vereinigten Staaten lahm zu legen. Mit einem Budget von weniger als zehn Millionen Dollar ausgestattet und geschickt auf die Knotenpunkte des weltweiten Rechnernetzes verteilt, könnte das Grüppchen Stromversorger abschalten, Flughafenkontrollen außer Kraft setzen und ein landesweites Chaos inszenieren.

Längst auch tummeln sich in den Netzen die Geheimdienste aus aller Welt. Der Bundesnachrichtendienst (BND) müht sich, „die vielfältigen Möglichkeiten der Kommunikation im Internet“ (BND-Vermerk) mitzulesen. Die Schnüffler erfassen E-Mails in der elektronischen Rasterfahndung und durchsuchen sie mit Hilfe von Wortbanken auf interessante Informationen. Und manchmal versuchen sie sich auch in direkten Angriffen.

Anfang 1998 machte eine Oldenburger Consulting-Firma mit dem Namen Padec GmbH einem 23 Jahre alten Hacker im Berliner Hotel am Bahnhof Zoo Avancen. Man benötige für einen Investor Informationen über die Datennetze in Iran. Auf einem Firmenbogen waren die Aufträge notiert: Welche Rolle spielt das iranische Postministerium, wer betreibt die iranische Bodenstation für den Satellitenzugang zum kuweitischen Provider?

Doch hinter der Firma standen keine Manager, sondern Geheimdienstmänner: Wenn es ihm gelänge, sich in die geheimen Computerprogramme der Mullahs einzuloggen, lockten die BND-Mannen den Hacker, gebe es richtig Geld. Besonders sei man an Informationen über Massenvernichtungswaffen interessiert. Ein Staatsanwalt, da könne er sicher sein, garantiere Straffreiheit für den Hack im Interesse der nationalen Sicherheit. Er könne seinem Land einen wertvollen Dienst erweisen. Der Student lehnte ab, kurz darauf verschwand auch die Padec GmbH.

Immer rascher hat die Gefährdung der Computerwelt in den vergangenen Jahren zugenommen. Anfang der achtziger Jahre konnten sich allenfalls Science-Fiction-Autoren oder Hollywood-Regisseure wie im Film „War Games“ Attacken auf die vernetzte Welt vorstellen.

Zwar gab es Hacker wie Kevin Mitnick, die sich in Computer- und Telefonnetzwerke einschleichen und Schaden anrichten konnten, doch deren Auswirkungen blieben begrenzt. Firmen, Behörden und private Computernutzer waren noch nicht über das Internet zusammengeschlossen, und Viren waren höchstens als akademisches Problem bekannt – aufgeworfen schon im Jahre 1949 durch den Computerpionier John von Neumann.

Erst 1986 wurde es ernst. Damals entwickelten die beiden aus Pakistan stammenden Programmierer Basit und Amjad Farooq Alvi erstmals eine Software, die sich im Computer selbständig fortpflanzen konnte. In Anlehnung an die Natur bezeichneten sie ihr Werk als Virus und tauften es „Brain“ („Gehirn“).

Das merkwürdige Programm, das auf Disketten kopiert wurde, tauchte vor allem an der Universität von Delaware in den USA auf und war eigentlich völlig harmlos – es benannte nur das Inhaltsverzeichnis aller vom Virus befallenen Disketten um in „Brain“.

Doch schon bald nahmen sich europäische Hacker des putzigen Stücks Software an. Im Dezember des gleichen Jahres präsentierte der Informatiker Ralf Burger auf der Konferenz des Hamburger Chaos Computer Clubs ein Virus namens „Virdem“.

VIRUCILLIN
Tarnt sich als Anti-Viren-Programm, legt 500 neue Unterverzeichnisse an

Zwei Jahre später sorgte ein elektronisches Biest mit dem Namen „Cascade“ in Textverarbeitungsprogrammen dafür, dass die Buchstaben einer gerade geöffneten Seite auf dem Bildschirm ins Rutschen gerieten und sich schließlich am unteren Rand des Monitors zu einem kümmerlichen Häufchen sammelten. Cascade vernichtete Hausarbeiten von Studenten und Artikel von Journalisten. Doch auch das sollte nur ein harmloser Anfang sein.

Anfang der neunziger Jahre übernahmen Hacker in Russland und Bulgarien unter Tarnnamen wie „Dark Avenger“ („Dunkler Rächer“) die Führung und entwickelten erstmals wirklich aggressive Computerschädlinge. Zudem nahmen ihre Erreger ausgeklügelte Formen an und konnten sogar ihr Aussehen und ihre Struktur selbständig ändern. Allerdings

„Wozu noch Atombomben?“

Geoffrey Baehr, 44, Netzwerk-Chef bei Sun Microsystems, über Cyber-Söldner, elektronische Kriegführung und die Gefahren für Zivilisten

SPIEGEL: Welche Rolle spielen Virus- und Wurmattacken im Alltag Ihrer Computerfirma?

Baehr: Wir erleben ständig die raffiniertesten Angriffe von Leuten, die versuchen, in unser Firmennetz einzubrechen oder einen bestimmten Rechner in die Knie zu zwingen. Wir zählen 350 bis 400 unterschiedliche Angriffsmethoden – und das sind nur die gebräuchlichsten. Auch die privaten PC-Benutzer werden in Zukunft wahrscheinlich sehr heftigen Bombardements ausgesetzt werden.

SPIEGEL: Wie sieht die Bedrohung für den privaten Computernutzer aus?

Baehr: Weil das Internet langsam und unbemerkt in den Alltag hineinwächst, werden die Folgen von Virusattacken immer gravierender. Da zunehmend Geräte wie Alarmanlagen und Handys ans Netz angeschlossen werden, greifen die Computerpiraten auch in den Alltag ein. Dem Normalbürger fällt das zunächst nicht auf, weil Web-fähige Handys wie normale Mobiltelefone aussehen. Tatsächlich aber sind die Geräte jetzt dem Datenstrom im Internet und damit Cyber-Attacken ausgesetzt. Und indem alles mit allem immer feiner vernetzt wird, steigt die Wahrscheinlichkeit, dass selbst ein simples natürliches Versagen ganz unschuldige Nutzer ernsthaft schädigen wird. Es kommt zu Fehlfunktionen, die totale Datensicherheit ist in der vernetzten Welt kaum mehr möglich.

SPIEGEL: Was könnte denn eine Cyber-Attacke gegen Handys oder Alarmanlagen anrichten?

Baehr: Ein Angriff muss sich gar nicht explizit gegen diese Geräte richten. Ihr Zusammenbruch wäre eine Nebenwirkung der eigentlichen Attacke. Eine Art GAU, den man sich leicht vorstellen kann: Es ist Freitagnachmittag, eine Stunde bevor die Börse an der Wall Street dichtmacht. Ein Angreifer schleicht sich ins Telefonsystem der amerikanischen Ostküste und lässt es zusammenbrechen. Der Aktienmarkt kollabiert. Aber das schlimmere Problem läge in den nicht geplanten Folgen: Der normale Bürger kann weder die Feuerwehr rufen noch einen Krankenwagen oder die Polizei. Die Energieversorgung und die Flugzeugkontrolle brechen zusammen – und noch mehr Systeme, die alle über dasselbe Netz laufen.

C&I

Konzernzentrale, Manager Baehr: *Piraten im Alltag*

SPIEGEL: Lebenswichtige Systeme sind genau aus diesem Grund auf private Netze beschränkt.

Baehr: Das Internet hat aber eine zusätzliche Eigenschaft, die selten in diesem Zusammenhang diskutiert wird: Es ist billig, weil so viele verschiedene Arten von Daten über dieselben Drähte und Leitungen transportiert werden können. Der ökonomische Vorteil, auch die Datenströme aus privaten Netzen mit anderen im Internet zusammenzufassen, ist sehr, sehr verlockend.

SPIEGEL: Wird es in Zukunft mit der elektronischen Aufrüstung und den hierauf spezialisierten Einheiten bei Geheimdiensten, Polizei und Militär nicht leichter, die Täter zu fassen?

Baehr: Auch in Zukunft wird die Strafverfolgung unter einem grundsätzlichen Problem der Cyber-Kriminalität leiden: Der Angreifer kann zu Hause oder in seinem Uni- oder Regierungsbüro sitzen – ganz anders als in der physischen Welt, wo der Einbrecher ein echtes Türschloss knacken und hoffen muss, dass ihn niemand dabei erwischt. Der Cyber-Terrorist kann unbemerkt über Jahre hinweg die Türen öffnen, jeden Tag ein Stückchen weiter.

SPIEGEL: Und solches Beharrungsvermögen trauen Sie jenen jungen Hackern zu, die sich vor allem mit dem Basteln von Viren zu beschäftigen scheinen?

Baehr: Solche Jungs wird es immer geben. Daneben werden wir es mit bezahlten Angreifern zu tun bekommen, eine Art Cyber-Söldner entsteht.

SPIEGEL: Die im Auftrag feindlicher Staaten die Vereinigten Staaten elektronisch bekämpfen?

Baehr: Das könnte durchaus sein. Hier in den USA wird das Problem jedenfalls sehr ernst genommen. Es existieren spezielle Abteilungen beim FBI und im Justizministerium, die sich nur mit Cyber-Kriminalität beschäftigen. Die westlichen Regierungen zumindest sind beunruhigt, sie arbeiten bereits an der elektronischen Kriegführung. Im Kosovo-Krieg etwa war eine US-Spezialeinheit gegen die serbischen Computersysteme im Einsatz. Als nächsten Schritt wird es automatisierte Gegenschläge geben.

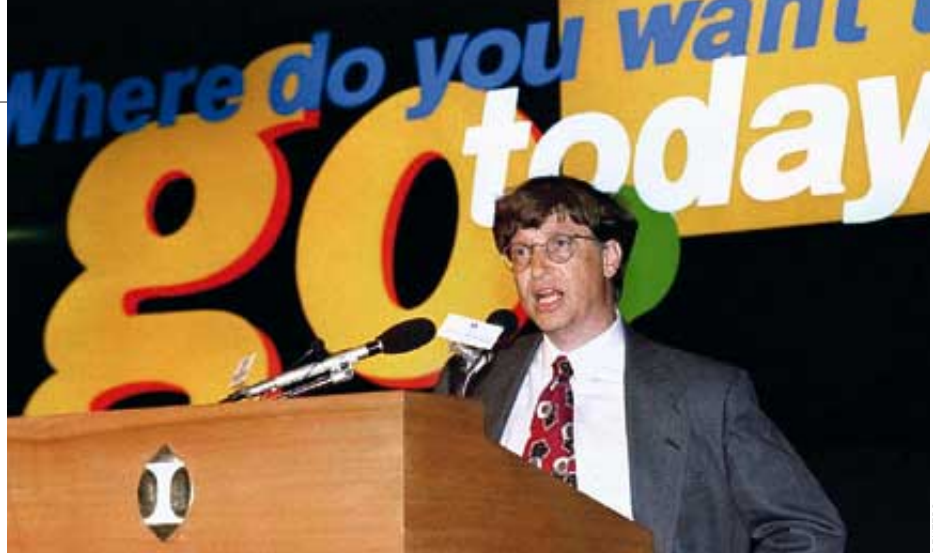
SPIEGEL: Wie stellen Sie sich das vor?

Baehr: Zum Beispiel könnten die Rechner einer gegnerischen Regierung versuchen, die Computer unseres Landes zu überfluten. Die entdecken aber, was da im Gange ist, analysieren, wer den Datenstrom losgelassen hat, und schicken dem Absender automatisch solche Datenmassen, dass diese Flut wiederum den Widersacher außer Kraft setzt.

SPIEGEL: Sie glauben, die Militärs entdecken das Internet als neues Spielzeug?

Baehr: Da bin ich mir ziemlich sicher. Das ist ein Krieg, der niemals erklärt wird, den jeder führen kann und dem wegen der globalen Vernetzung im Prinzip jeder zum Opfer fallen kann. Und einer, der sehr billig ist, sowohl für gegnerische Länder als auch für terroristische Gruppen. Warum sollte man noch die Anstrengung unternehmen, Atomwaffen zu bauen? Es ist so viel billiger, ein paar Informatiker einzustellen.

Interview: Rafaela von Bredow



REUTERS

Microsoft-Chef Gates: *Warnung vor staatlicher Einflussnahme*

blieb die Zahl der Software-Schädlinge vorerst noch überschaubar. Allenfalls 300 verschiedene Viren registrierten die Experten Anfang der neunziger Jahre. Nur 24 Monate später hatte sich deren Zahl jedoch bereits verzehnfacht. Hacker wie „Nowhere Man“ und „Dark Angel“ hatten so genannte Construction Kits veröffentlicht, die es auch weniger talentierten Programmierern ermöglichten, neue Viren zu konstruieren.

Massenepidemien blieben aus. Denn immer noch verbreiteten sich die meisten Viren nur über Disketten. So dauerte es Wochen, bisweilen sogar Monate, bis ein Schädling von einem Kontinent zum anderen schwappte.

Das änderte sich erst, als immer mehr Menschen das Internet entdeckten, heute sind 300 Millionen Menschen an dem großen Kommunikationsstrang angeschlossen. Erst jetzt können sich Viren explosionsartig vermehren.

MONOPOLY Spioniert User-Namen und E-Mail-Adressen aus, versendet sie an anonyme Mail-Accounts

Das programmierte Chaos im Netz und die illegalen Aktivitäten des Computer-Undergrounds beschäftigten rasch eine ganze Branche. Schon 1987 brachte die Anti-Virus-Industrie den ersten Virenscanner auf den Markt, eine Art elektronisches Diagnosegerät. Seitdem profitieren ihre Aktienkurse von jeder neuen Epidemie. Allein die Aktie des US-Konzerns McAfee sprang Anfang Mai, nach dem Auftauchen des Liebesbriefs aus Manila, um über 40 Prozent nach oben.

Nicht selten waren es ehemalige Hacker, die plötzlich die Seiten wechselten und Programme zur Abwehr ihrer früheren Kameraden schrieben, als handle es sich um einen sportlichen Wettkampf. Der hannoversche Hacker „Mixter“ etwa, Urheber des Programms, mit dem Online-Piraten im Februar die Internet-Konzerne attackierten, half Firmen bei der Abwehrtaktik gegen seine eigene Software.

Der wichtigste amerikanische Online-Helfer ist der 21-jährige frühere Hacker John Vranesevich, der mittlerweile mehr als 7000 Dossiers über aktive Computervandalen angelegt hat. Er ist, so das US-Magazin „Vanity Fair“, der „Sherlock Holmes des Internet“.

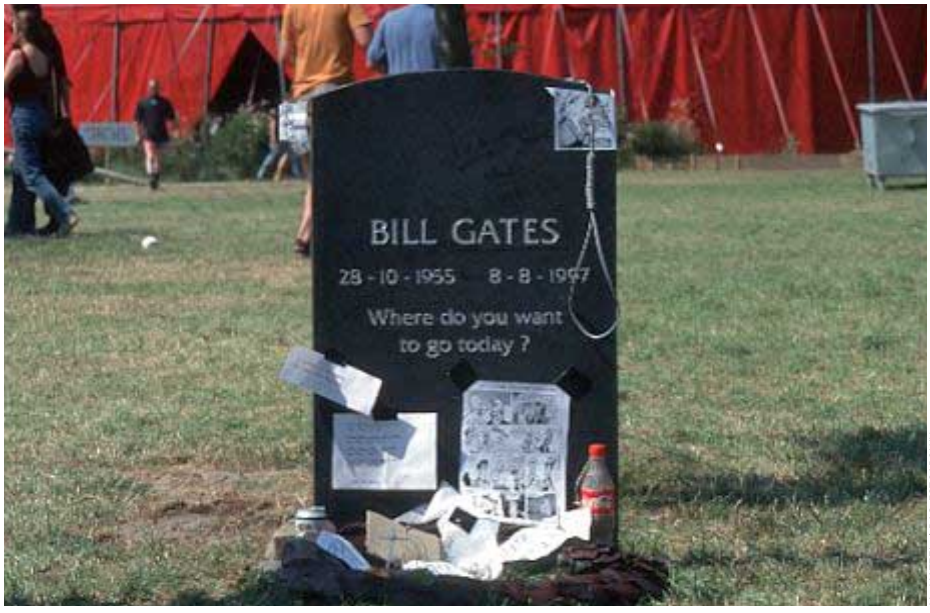
Viele Verantwortliche scheinen jedoch noch immer in den neunziger Jahren zu leben, als den Hackern ein Robin-Hood-Appeal anhaftete. Trotz der neuen machtvollen Bedrohung, so klagt etwa Charles B. Wang, Chef des Software-Konzerns Computer Associates und einer der führenden Software-Manager der Welt, „nehmen sie die Risiken immer noch nicht ernst“. Gerade mal 30 Prozent aller Firmen, so rechnen Experten, haben ständig Virenscanner und Sicherheitsprogramme wie die so genannten Firewalls im Einsatz.

Dabei hat sich die Computerwelt in einen bunten Mutantenzoo verwandelt. Marodierende Viren, Würmer, Hoaxes oder Trojanische Pferde gehören inzwischen zum Alltag im Cyberspace.

Um sich von den „script kiddies“ abzusetzen, die ihre Viren und Angriffswerkzeuge aus Online-Baukästen zusammensetzen, produzieren die erfahrenen Hacker immer bösartigere Programme – mit möglichst weltweiter Sprengkraft. Während etwa Viren bis vor kurzem ausschließlich Software oder digitale Daten vernichten konnten, zerstören sie inzwischen sogar die Hardware des Rechners.

So verbreitete im vergangenen Jahr ein taiwanischer Programmierer namens Chen Ing-Hau Angst mit einem Eindringling, den er nach seinen Initialen CIH nannte. Das als Zeitbombe konstruierte Virus, das auf den infizierten Computern erstmals am 26. April 1999 platzte und inzwischen diverse Abarten entwickelt hat, zerstört den Startmechanismus und löscht die Festplatte – der GAU in der Computerwelt.

Um den Computer wieder anschalten zu können, muss ein neuer Bios-Chip eingebaut werden, aber selbst danach sind sämtliche Daten und Programme unwiederbringlich verloren. „Erstmals“, staunten die Fachleute der Software-Firma Sophos, „haben wir es mit einem Virus zu tun, dessen Wirkung nur durch das physikalische Öffnen des Rechners und das Ersetzen einer Komponente geheilt werden kann.“ Trotz zahlreicher Warnungen, so schätzen Experten, verwandelte CIH weltweit bereits mehr als 50 000 PC zu Schrott. All diese Schläge unter die



M. MATZEL / DAS FOTOARCHIV

Mahnmal von Microsoft-Gegnern: *Monokulturen sind anfällig*

L. PSIHOYOS / MATRIX / AGENTUR FOCUS

Sun-Chef McNealy
Kampf den Viren und Würmern

Gürtellinie sind nach Meinung von Experten aber erst der Anfang. „Der Love-Virus war ein Schuss vor den Bug aller Internet-Nutzer“, sagt etwa Hans-Peter Martykan, Sicherheitsexperte beim Münchner Versicherungsriesen Allianz.

„Wir haben bisher noch Glück gehabt“, glaubt auch Karl Altmann. „Genauso gut“, meint der Deutschland-Chef der amerikanischen Anti-Viren-Firma Finjan, „hätten die Hacker mit dem Liebesbrief auch ein weit bösartigeres Programm verschicken können.“

Als eine der größten Bedrohungen sieht Altmann die Trojanischen Pferde, die dem Hacker durch die Hintertür Zugang in quasi jeden PC verschaffen. Der bekannteste Trojaner dieser Art wurde von der kalifornischen Hackergruppe „Cult of the Dead Cow“ (cDc) entwickelt, einer der machtvollsten Gangs im Cyberspace. Unter dem Namen „Back Orifice“ („Hintere Öffnung“) ist es seit fast zwei Jahren im Internet für jedermann kostenlos verfügbar.

Mehrfach schon wurde das Spionageprogramm modernisiert und von anderen Virenautoren weiterentwickelt. Doch allein die Ursprungsversion, so schätzen Experten, wurde am Erscheinungstag von rund 14 000 Interessenten abgerufen; inzwischen wurde es mehr als 100 000-mal von der cDc-Seite heruntergeladen.

„‚Back Orifice‘“, meint Experte Altmann, „ist der Traum jedes Hackers und der Alptraum jedes Internet-Surfers.“ Gelingt es dem Hacker, die Spionagesoftware, etwa per E-Mail und einer angehängten Datei, auf den Rechner eines Opfers zu schmuggeln, dann hat er dort fast unbeschränkte Möglichkeiten, denn der Trojaner erledigt alle Installationsarbeiten heimlich und selbständig.

Geht das Opfer online, meldet sich „Back Orifice“, ohne dass der Nutzer es merkt, per E-Mail bei dem Hacker. Ohne größere Programmierkenntnisse kann der Eindringling dann von jedem Punkt der Erde sehen, was gerade bei seinem Opfer über den Monitor flimmert. Er kann mitlesen, welche Briefe der PC-Benutzer schreibt, und feststellen, welche Passwörter oder Geheimnummern er benutzt, um sich bei seiner Online-Bank oder bei einer Firmendatenbank einzuloggen.

MELTING SCREEN
Als Bildschirmschoner getarnt, benennt Programme um, stört Bildschirm

Solange der PC-Nutzer online ist, wird jede Tastatureingabe protokolliert. Bei der Eingabe von PIN-Nummern erkennt der Spion auf seinem Bildschirm sogar die Zahlen, während der Bankkunde nur Sternchen sieht. Ist der PC technisch gut ausgerüstet und verfügt über Kamera und Mikrofon, dann kann der Hacker seinem Opfer quasi über die Schulter gucken und mithören, was er gerade mit Kollegen bespricht. „Da wird die Schreckensvision von Big Brother wahr“, meint Altmann.

Dabei ist das Virus der toten Kühe aus Kalifornien längst nicht mehr das Einzige, das aus einer Möglichkeit, die ursprünglich für Systemadministratoren zur Überwachung und Wartung der Netzwerke in großen Firmen gedacht war, ein höchst effizientes Spionagewerkzeug macht. Zahlreiche Ableger wie „Backdoor-G“, „Net-

Der Weg der Viren in den Computer

E-MAIL
Häufigster Übertragungsweg ist heute die elektronische Post. Dabei versteckt sich das Virus in einer angehängten Datei. Wird der Anhang per Doppelklick aktiviert, startet es seine zerstörerische Arbeit.

INTERNET
Moderne Internet-Seiten mit multimedialen Inhalten und Werbebannern arbeiten oft mit dem Software-Modul „ActiveX“, das alle Macht im Computer übernehmen kann. Statt einer Animation kann mit dem Klick auf ein Bildschirmsymbol auch ein Virus übertragen werden.

DATENTRÄGER
Über infizierte Disketten oder CD-Roms gelangen die Viren auf die Computer-Festplatte. Die Ausbreitungsgeschwindigkeit ist relativ gering. Dieser Weg spielt heute eine untergeordnete Rolle.

Der Schaden

Dateien können versteckt, verändert oder ganz gelöscht werden.

Computerprogramme können beeinträchtigt oder manipuliert werden.

So genannte „Trojanische Pferde“ geben Hackern Einblick in fremde Computer.

Durch automatisch ablaufende Kettenbrief-Aktionen können Netzwerke lahmgelegt werden.

Die Abwehr

FIREWALL
Mit spezieller Sicherheitssoftware können Unternehmen dafür sorgen, dass bereits bekannte Viren gar nicht erst die Firmen-PC erreichen. Rechner mit besonders sensiblen Datenbeständen bilden ein in sich geschlossenes Netz ohne Verbindung zum Internet.

ANTI-VIREN-PROGRAMME
So genannte Virenscanner können anhand bestimmter Dateistrukturen bekannte Viren erkennen, Alarm auslösen und den Schädling vernichten. Da sich die Zahl der Viren ständig erhöht, muss der Virenscanner mindestens monatlich aktualisiert werden.

VOM NETZ TRENNEN
Wer ständig online ist, läuft schneller Gefahr, Opfer von Hackerattacken zu werden. Computer ohne Internet-Zugang können nur durch CD-Roms oder fremde Disketten verseucht werden.

DER SPIEGEL

O. LAUDE / LIAISON / SIPA PRESS

Linux-Erfinder Torvalds: *Plädoyer für mehr Konkurrenz*

bus“ oder „Sub7“ sprechen für die Beliebtheit der illegalen Hinterschlüssel. Und sie werden immer umfangreicher.

„Sub7“ zum Beispiel, das der Virenjäger Alexej Podrezow von der finnischen Software-Firma F-Secure für „die am besten entwickelte Hintertür“ ansieht, verfügt über mehr als hundert Funktionen, mit denen der Hacker sein Opfer ausspionieren oder schlicht narren kann – etwa, indem er per Fernsteuerung den Mauszeiger versteckt, die Bildschirmfarben ändert oder einfach den Computer ausschaltet.

Wie weit das Spionageprogramm, das zurzeit nur auf Windows-PC funktioniert, bereits wirklich für kriminelle Zwecke eingesetzt wird, ist unter Experten umstritten. Microsoft-Manager versuchen eifrig, das Problem herunterzuspielen.

Auch die meisten Anbieter von Anti-Viren-Programmen glauben, dass sie das Problem im Griff haben. Da die bekannten Formen des Trojaners von den meisten Schutzprogrammen erkannt werden, stufen sie das Risiko der Infizierung lediglich als „mittel“ (McAfee) bis „schwach“ (Sophos) ein.

Andere Experten wie Finjan-Chef Altmann dagegen rechnen mit einer ansehnlichen Dunkelziffer, besonders weil sich die meisten Opfer scheuen, offizielle Ermittler einzuschalten. So glauben etwa amerikanische Computerspezialisten, schon heute seien „einige zehntausend PC“ mit einem Hinterschlüssel zugänglich. Indizien sprechen sogar dafür, dass die Backdoor-Programme ihre Opfer zumindest eine Zeit lang automatisch an eine zentrale Web-Adresse in den USA gemeldet haben.

Aber nicht nur bösartige Eindringlinge bereiten den Sicherheitsexperten Sorgen. Schon die allerorten im Netz eingesetzten Techniken, mit denen die Internet-Anbieter ihren multimedialen Schnickschnack verbreiten oder mit denen die Software-Firmen den Kunden den Umgang mit dem Computer erleichtern, bilden ein ideales Biotop für verheerende Mikroorganismen. Ohne zu wissen, was sich hinter den poppigen Animationen, hinter Werbebannern und bunten Bildern versteckt, klicken die meisten Surfer bedenkenlos auf alles Mögliche.

Doch den wenigsten ist bewusst, was der Klick auf ein Bildschirmsymbol bewirkt:

TEQUILA Getarnt durch aufwendige Verschlüsselung, infiziert „.exe“-Dateien, stört Monitor mit Fraktalbild

Er ruft nicht selten ein Software-Modul namens „ActiveX“ auf, das im selben Moment alle Macht im Rechner übernimmt. Reines Glück, wenn es wirklich nur die versprochene Animation präsentiert; ebenso gut könnte es binnen Sekunden alle gespeicherten Daten demolieren. Selbst das von manchen Anbietern vorausgeschickte Sicherheitszertifikat besagt kaum etwas. Jeder, der noch nicht öffentlich als Hacker aktenkundig geworden ist, kann es für ein paar Mark erwerben.

Was auch immer der Benutzer wählt, es ist falsch. Vernünftig wäre es, all die kleinen, gefährlichen Programme abzublocken, die in vielen Webseiten verborgen sind, nur um dort Bilder aufblinken oder Animationen ablaufen zu lassen. Praktikabel ist es nicht. Wer sich dem Treiben verweigert, bleibt alle naselang beim Online-Surfen stecken. Immer wieder erscheinen Warnfenster und belästigen den Nutzer mit Anfragen, zuweilen bleibt der Bildschirm schlicht leer. Die Online-Fahrt mit dem Computer würde aussehen wie ein Film, der alle paar Sekunden angehalten würde.

Eine Patentlösung gegen Feldzüge aus dem Cyberspace gibt es nicht. Weltkonzerne wie Siemens oder die Allianz, die täglich mit Kunden, Lieferanten und Mitarbeitern rund um den Globus kommunizieren, können sich abgeschottete Systeme nur in Teilbereichen leisten. Allianz-Manager Martykan und sein Siemens-Kollege Kampffmeyer überlegen deshalb, wie sie zusätzliche Sicherungen gegen die Bedrohungen aus der Online-Welt einbauen können.

Doch das Sicherheitsbedürfnis kollidiert hier, wie bei den meisten anderen Firmen auch, mit dem Hang zur Bequemlichkeit. Schon heute stöhnen Computerbenutzer über jedes zusätzliche Codewort, das sie eingeben müssen. Solche Schotten bremsen nicht nur das Arbeitstempo, sondern belasten zudem auch noch die Zentralcomputer der Firmen: „Irgendwann“, fürchtet Kampffmeyer, „kommen die Angestellten vor lauter Schutzmaßnahmen nicht mehr zum Arbeiten.“

Clevere Hacker, das wissen die EDV-Manager nur zu gut, werden auch künftig Mittel und Wege finden, wie sie die Netze von Behörden oder Konzernen angreifen können. Vor allem gegen die Datenbombardements, die im Februar Internet-Seiten von Yahoo, eBay und anderen Online-Konzernen lahm legten, gibt es kaum eine Abwehr. Anders als frei flottierende Viren können sie nicht mit einem digitalen Antibiotikum neutralisiert werden.

„Es gibt im Grunde nichts, was eine Internet-Seite davor schützen könnte, zum Opfer einer koordinierten Netzwerk-Attacke zu werden“, warnte eine von der US-Regierung bezahlte Experten-Gruppe in einem Anfang April veröffentlichten Bericht.

Um wenigstens die rasch um sich greifenden Virenepidemien besser eindämmen zu können, meint Eric Chien, Leiter des europäischen Forschungsteams von Symantec, müssten sich in Zukunft vor allem die Internet-Provider selber stärker um den Schutz kümmern.

Damit läge die Verantwortung für den Virenschutz nicht mehr nur bei den überforderten Endnutzern. Verdächtige Dateien würden vom Netzbetreiber als „gefährlich“ markiert und automatisch als Kopie in Quarantäne gebracht – eine Technik, die als „Clean Pipe“ bezeichnet wird, weil sie die „Rohre“ für den Informationsfluss sauber hält.

Doch bislang sind solche Ideen nur eine Vision. Experten rechnen deshalb damit, dass sich das Problem durch den Internet-Boom – täglich loggen sich über 100 000 neue Nutzer ein – und neue Techniken rasch verschärfen wird.

Jan Knop, Leiter des Rechenzentrums der Universität Düsseldorf und einer der Mitglieder des Aksis-Kreises, urteilt: „Die Bedrohung für Deutschland ist riesig, und sie wird leider immer weiter wachsen. Jeder Einzelne wird verletzlicher, vor allem auch in seiner Privatsphäre."

Handys und Organizer

Neue superschnelle Breitband-Verbindungen in die Online-Welt werden es den Piraten viel einfacher machen, Computer zu kapern. Die Rechner sind bei dieser neuen Technik permanent an das Datennetz angeschlossen und wählen sich nicht, wie heute üblich, jedes Mal neu ins Netzwerk ein. Schon in den nächsten drei Jahren wird die Zahl der Breitbandanschlüsse über Kabelmodem allein in den USA von 1,35 auf 9 Millionen steigen.

Dazu werden mehr und mehr Geräte entwickelt, die sich automatisch ins Netz einwählen, um Informationen abzurufen – wie etwa der per Wetterbericht gesteuerte Rasensprenger, Web-Fernseher oder Web-Telefone – willkommene Opfer für Hacker, die auf den wenig überwachten Prozessoren ihre teuflische Angriffssoftware installieren könnten.

Auch Handys könnten bald schon zum Ziel für Hacker werden. So genannte SMS-Bomben, die kürzlich erstmals entdeckt wurden, lassen schon die ersten Gefahren erkennen. Mit diesem elektronischen Spielzeug, einem hinterhältigen Programmfetzen, ist es möglich, per Internet fast jedes Handy zu überfluten, indem es hunderte von Kurznachrichten auf jede gewünschte Telefonnummer schickt.

Virenattacken auf Handys und Organizer, so glauben Sicherheitsexperten, werden bald folgen. Hacker vermuten, dass in ihren Kreisen bereits an vielfältigen Plagen für die kleinen Kommunikationscomputer gearbeitet wird. „Ich kenne einige Leute", meint ein Hacker mit dem Tarnnamen „RadwOrk", „die sich damit befassen würden – und sei es nur, um auszuprobieren, was passiert."

Doch nicht nur Hacker werden ihre Künste an den neuen Geräten ausprobieren. Auch ernsthafte Kriminelle dürften ihre Aktivitäten mehr und mehr ins Netz verlagern. Schon jetzt bietet das World Wide Web Ganoven nahezu unbegrenzte Möglichkeiten für Erpressung und Sabotage, Waffen-, Drogen- und Menschenhandel, für Betrug und Geldwäsche.

BABYLONIA
Aktualisiert sich selbst per Internet, zerstört Dateien, versendet sich über Chats

Während die Möglichkeiten nationaler Ermittlungsbehörden an den jeweiligen Staatsgrenzen enden, hat der Internet-Gangster in ein paar Sekunden den Erdball umrundet. Und was in dem einen Land strafbar ist, muss in dem anderen längst nicht verboten sein.

Die Ermittlungsbehörden sind mit den Hightech-Verbrechen ohnehin überfordert. Die Philippinen, Ursprungsland des Liebes-Virus, haben wie viele aufstrebende Staaten noch nicht einmal Gesetze gegen Computerkriminalität. Doch auch in Europa und Amerika fehlt es allerorten an geschulten Fahndern.

„Wir werden die Verantwortlichen finden und vor Gericht bringen", hatte Anfang Februar noch die amerikanische Justizministerin Janet Reno den Hackern zugerufen, die mit ihren Attacken die führenden Internet-Firmen des Landes lahm gelegt hatten. Doch bis heute gelang es lediglich, den kanadischen Teenager mit dem Screennamen „Mafiaboy" zu fangen, der sich durch sein Geprahle in Online-Chatrooms selbst verraten hatte.

Oft hapert es schlicht an der Technik. Während die Polizei in Deutschland, wenn auch nur auf richterlichen Beschluss, jedes Telefon abhören kann, ist die Überwachung des E-Mail-Verkehrs in Echtzeit nahezu unmöglich. Dazu dürften zurzeit lediglich Geheimdienste mit ihren riesigen elektronischen Ohren und Computergehirnen wie der US-Abhörstation Echelon im bayerischen Bad Aibling fähig sein.

Auch die Nestlé-Erpresser, die am 28. Dezember festgenommen wurden, hätten schon sehr viel früher gefasst werden können, „wenn wir über bessere Technik verfügt hätten", klagt der EDV-Sachverständige Rainer Richard aus dem Polizeipräsidium München. Rund 200 Nachrichten hatten der ehemalige Manager Michael S. und seine Ehefrau Christine als „Robin Food" auf elektronischem Weg an den Frankfurter Nestlé-Konzern verschickt und darin acht Millionen Mark gefordert. Doch die Fahnder konnten den Absender einfach nicht identifizieren.

Zum Schein ging der Konzern schließlich auf die Forderungen ein und überwies, streng nach E-Mail-Anweisung, einen Betrag nach Riga in Lettland. Von dort wanderte das Geld zur Hamilton-Bank im Karibik-Paradies Grenada, weiter nach Zypern und schließlich nach München – auf das Konto der Erpresser. Dumm gelaufen, denn die Polizei klebte, das war ihre einzige Chance, von Anbeginn an jedem

Steuerzentrale eines Industriebetriebs im Ruhrgebiet: *„Die Bedrohung für Deutschland ist riesig"*

H. D. ZINN / LAIF

Transfer. Der kriminelle Quantensprung war, diesmal noch, missglückt.

Oft stoßen die Ermittler auch noch auf eine Schweigemauer bei den Betroffenen. An neuen Gesetzen oder verschärfter Aktivität der Gesetzeshüter sind die meisten Konzerne gar nicht interessiert. Sie wollen das Problem lieber mit Hilfe privater Online-Detektive und Sicherheitsfirmen lösen. Jedes Gerichtsverfahren gegen einen Hacker würde sie zwingen, ihre Sicherheitslücken zu offenbaren, und dadurch nicht nur Nachahmer animieren, sondern auch Kunden abschrecken.

Ende Februar warnte deshalb der Sicherheitschef des Microsoft-Konzerns, Howard Schmidt, den amerikanischen Kongress bei einem Hearing vor „unnötiger Regulierung und Einflussnahme auf die Operationen dynamischer und sehr produktiver Geschäftsbereiche“. Und auch Linux-Schöpfer Linus Torvalds sowie Scott McNealy vom Computerkonzern Sun wünschen sich von der Regierung Bill Clintons keine allzu dirigistischen Eingriffe.

Charles Giancarlo, Vizepräsident des Cisco-Konzerns, behauptet sogar: „Die Industrie hat gezeigt, dass sie rasch die Angreifer zurückschlagen und die nötigen Maßnahmen ergreifen kann, damit ähnliche Attacken künftig nicht so einfach gelingen.“

Wie lange das noch gelingt, ist fraglich. Dass die Mafiabanden aus Russland und die Paten aus Sizilien nicht schon heute das Netz in großem Stil nutzen, liegt nach Meinung von Fahndern vor allem daran, dass sie die gigantischen Möglichkeiten des neuen Mediums noch nicht begriffen haben. Bis der Generationswechsel vollzogen ist, läuft für Firmen und Ermittlungsbehörden noch eine Gnadenfrist.

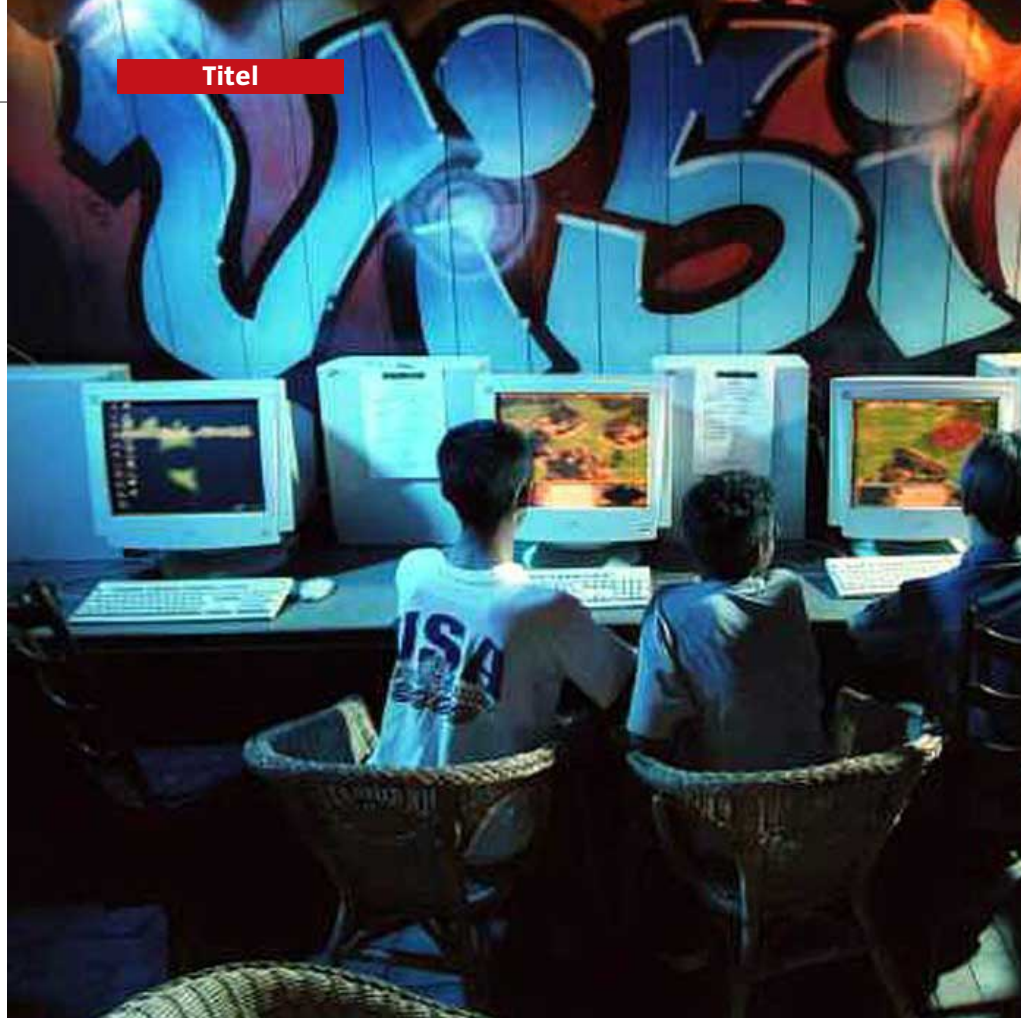
Doch dann, so glaubt etwa Edwin Kube vom Bundeskriminalamt, könnte vielleicht sogar das perfekte Verbrechen möglich werden. Ein mögliches Szenario: Der Täter klinkt sich in den Rechner einer Klinik ein und manipuliert die Medikamenten-Dosierung eines Intensivpatienten.

Nach Ansicht mancher Computerexperten sind solche Überfälle schon heute möglich. Schon vor Jahren, so berichteten vergangene Woche deutsche Hacker, hätten sie sich in Klinikrechner eingeklinkt, um die Patientendossiers zu manipulieren – „just for fun“.

Ein Hacker: „Stellen Sie sich das Gesicht eines Patienten vor, dem am nächsten Tag irrtümlicherweise ein Tumor attestiert wurde.“

Wirklich überprüfbar sind solche Schilderungen nicht. Doch der amerikanische Computeringenieur Mike Chisina von der Firma Network Security Technologies ist sich mit vielen Experten einig: „Science-Fiction ist heute.“

Dinah Deckstein, Manfred Dworschak, Klaus-Peter Kerbusk, Georg Mascolo, Mathias Müller von Blumencron, Andreas Ulrich



Internet-Café „Falkens Maze“ in Fürth: *„Die meisten sitzen in Haft, sind ausgewandert oder*

„Einmal Gott sein“

Jahrelang polierte die Hackerszene das eigene Robin-Hood-Image. Seit dem „I love you“-Virus ist klar: Der neuen Generation geht es vor allem um Zerstörung. Die einst verschworene PC-Gemeinde ist zersplittert und eitel, geldgierig und machtversessen.

Das Leben von Andy Zauner, 22, begann mit einem Amiga. Er erinnert sich noch genau. Damals war er zehn, und das Plastik-Ungetüm aus der Computer-Urzeit wurde sein Schlüssel zu einer neuen Welt. Nur welche?

Später bekam er einen 386 SX 16, dann einen 486 DX 50, irgendwann das erste Modem. Da war er 13, und das Modem wurde sein Tor zu allen Datennetzen dieses Planeten. Nur, was sollte er dort?

Mit 16 mietete sich Andy in seinem Heimatnest Ingolstadt ein Kellerloch an, in dem irgendwann 50 PC rumstanden – mit 30 ISDN- und 42 Analog-Leitungen. Telefongebühren fielen nicht an, wenn man sich mit „Blueboxing“ auskannte, einem akustischen Trick, die Gebührenimpulse auszuschalten. Obendrein konnte sich der Gymnasiast rühmen, die größte Raubkopier-Mailbox Europas zu betreiben.

Doch eines Tages klingelten ein paar Polizeibeamte bei ihm zu Hause. Da war den Zauners endgültig klar, dass ihr Sohn Karriere machen würde. Aber als was?

Als Vorstandsvorsitzender einer Internet-AG oder als Knast-Stammkunde?

Andys Eltern waren besorgt – durchaus zu Recht, denn ihr Sohn war zum Hacker mutiert. Und Hacker, das wussten sie aus der Zeitung, sind vereinsamte, picklige bis psychopathische Kriminelle, die schon mal aus Versehen einen Atomkrieg auslösen könnten wie in dem Film „War Games“. Seither sind sechs Jahre vergangen, und in der Szene hat sich nicht nur der Kinokult verändert.

Heute taugt der Krieg spielende Zauberlehrling dem Nachwuchs weit weniger zum Vorbild als die Hackerprofis in „Sneakers“, die für Abschirmdienste, Konzerne und viel Geld gegnerische Rechner knacken. Cyber-Söldner statt Schulbank-Chuzpe.