Fliegender Korsar

In einer Großrazzia hob das FBI ein Dutzend US-Kinderzimmer aus: Jugendliche Computer-Eindringlinge („Hacker") haben sich in die Datennetze zahlreicher Großfirmen und sogar des Pentagon eingeschlichen.

Um 8.30 Uhr morgens, am Mittwoch vorletzter Woche, klingelten sechs FBI-Beamte und zwei Sicherheitsexperten der Telephonfirma Bell an der Wohnungstür der Familie Stadjas in Detroit. Mrs. Sharon Stadjas öffnete: Haussuchung.

Die Beamten stürmten als erstes ins Kinderzimmer, wo Stadjas-Sohn Eric, 14, die Geräte für sein Hobby installiert hatte: einen Heim-Computer und etliche Zusatzapparate, mit denen er tage- und halbe Nächte lang umging. Die FBI-Beamten drehten Matratzen um, durchwühlten Schubladen, spähten unters Bett und konfiszierten Kladden und Computer-Broschüren.

„Erst wußte ich gar nicht, was das alles bedeuten sollte", sagt Mrs. Stadjas. Doch dann hätten die Beamten ihr erklärt, ihr Sohn stünde unter schwerem Verdacht: Er habe sich in das Datennetz des amerikanischen Verteidigungsministeriums eingeschlichen, habe dort „Daten gefälscht und verändert und Botschaften hinterlassen".

Wie bei Mrs. Stadjas in Detroit, so untersuchten US-Sicherheitsbeamte am selben Tag noch in mehreren amerikanischen Städten die Kinderzimmer und Bastelkeller von mehr als einem Dutzend jugendlicher Computer-Freaks – es war die erste Großrazzia der US-Behörden gegen Jugendliche, die per Heim-Computer in geheime Datenbanken „einbrechen". Nicht nur Privatfirmen, Banken und Institute, sondern auch die Experten des amerikanischen Verteidigungsministeriums sehen sich zunehmend von solchen unbefugten Computer-Schnüffeleien bedroht.

Wie bei Eric Stadjas, so beschlagnahmten die FBI-Beamten auch bei den anderen Familien alles Computer-Gerät und die einschlägigen Betriebsanleitungen und Aufzeichnungen. Alle Jugendlichen wurden verhört, verhaftet wurde keiner.

Denn bisher gibt es in den USA noch kein bundesweites Gesetz gegen derartigen Mißbrauch von Computern.

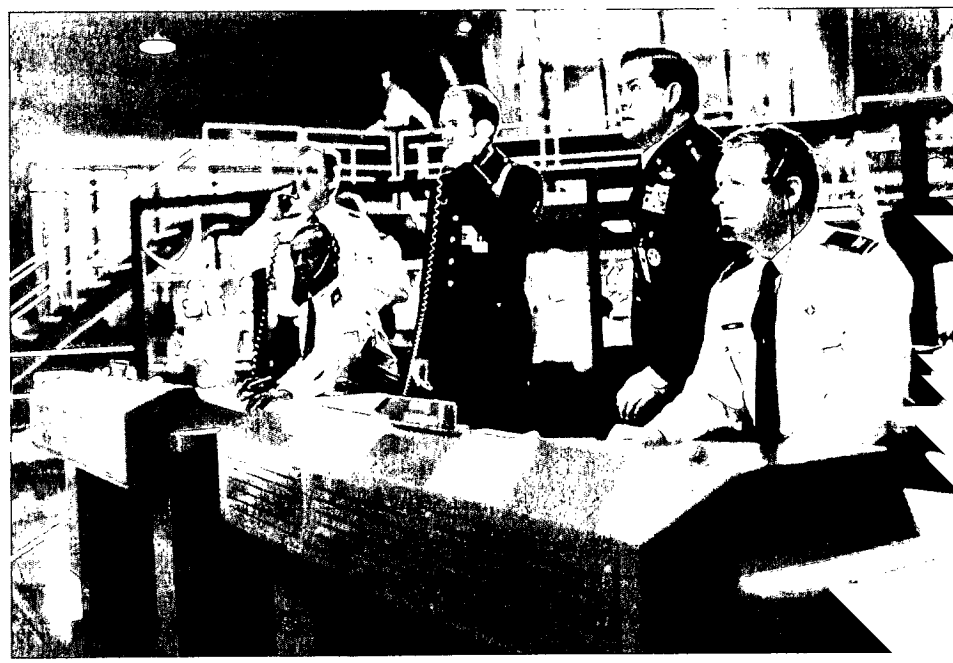
Erst Ende letzten Monats brachte der demokratische Kongreßabgeordnete Bill Nelson aus Florida eine Gesetzesvorlage ein: Freiheitsentzug bis zu fünf Jahren für Tatbestände wie unerlaubter Zugang zu Computern, Datendiebstahl oder Beschädigung des Speicherinhalts von Rechnern.

Bisher können die jugendlichen Computer-Fummler, in der einschlägigen Szene „Hacker" genannt, allenfalls zu Schadenersatz herangezogen oder wegen unbefugter Nutzung von Fernmeldeeinrichtungen belangt werden.

Experten befürchten, daß neue Gesetze gegen die Geisterfahrer in den Computer-Netzen nur wenig werden ausrichten können – während der mögliche Schaden für die Betroffenen wächst:

- ▷ 600 000 Heim-Computer, sechsmal so viele wie noch vor drei Jahren, sind gegenwärtig bei amerikanischen Familien in Gebrauch – eine kaum mehr überschaubare Zahl möglicher Täter. Schätzungsweise 180 000 Heim-Computer sind mit einem Zusatzgerät („Modem") ausgestattet, das über die Telephonleitung den Zugang zu staatenweiten Computer-Netzen eröffnet.
- ▷ Gleichzeitig ist die Zahl der sensiblen Daten, die in Computer-Systemen gespeichert und mehr oder minder miteinander vernetzt sind, ins Gigantische gestiegen. Allein im Bereich des Pentagon arbeiten schon mehr als 8000 Groß-Computer; täglich kommen neue hinzu. Und allein bei der amerikanischen Rüstungsindustrie gibt es schon mehr als eine Million Menschen, die für den Zugang zu geheimen Daten legitimiert sind. „Das", so Donald C. Latham, verantwortlich für Computer-Sicherheit im Pentagon, „ist die wahre Schwachstelle."
- ▷ Geringer als bei den meisten anderen Vergehen oder Verbrechen ist die

Computer-Eindringlinge Gary und Greg Knutson (M.)*: Geisterfahrer im Nasa-Netz



Computer-Thriller „War Games": Sabotage mit schlafenden Programmen?

* Mit Freunden bei einer Pressekonferenz in ihrer Schule am Donnerstag vorletzter Woche.

Chance der Entdeckung – nur in den seltensten Fällen hinterlassen Computer-Einbrecher Spuren oder „Fingerabdrücke", mit deren Hilfe sie überführt werden könnten.

Daß einzelne, besonders pfiffige Computer-Freaks sich unerlaubten Zugang zu fremden Daten verschaffen konnten, war den Experten schon in den 70er Jahren klargeworden. Inzwischen hat sich daraus fast eine Art amerikanischer Nationalsport entwickelt.

„Jede Oberschule und jede Universität, an der es Computer-Kurse gibt, hat auch etliche Jugendliche, die das betreiben", meint Donn B. Parker, Verfasser mehrerer Bücher über Computer-Kriminalität. Die Zahl derer, die sich an den elektronischen Streifzügen durch Computer-Netze beteiligen, wird in den USA auf einige tausend geschätzt. „Nur die wenigsten", so ein 19jähriger Computer-Student in Chicago, der sich im Datenaustausch mit Freunden „Mr. Xerox" nennt, „werden geschnappt, und natürlich auch nur die, die am wenigsten Ahnung haben."

Gefaßt wurde Mitte Juli eine Gruppe von Schülern im US-Staat Milwaukee, Teenager und Twens, die sich nach der Telephonvorwahl von Milwaukee „414er" nannten.

Über Monate hatten sich die jungen Leute von ihren Heim-Computern aus elektronischen Zugang zu 60 Großrechnern in den USA und Kanada verschafft. Sie waren beispielsweise in den Computer des New Yorker Sloan-Kettering-Krebs-Zentrums eingedrungen und hatten Daten über die Bestrahlungsdauer von Krebspatienten durcheinandergebracht; auch fanden sie Einlaß in ein (nichtgeheimes) Computersystem des Atomwaffen-Forschungszentrums in Los Alamos (US-Staat New Mexico).

Der Einstieg in die fremden Datensysteme gelang den Jugendlichen über das sogenannte „Telenet", einen kommerziellen Datenverbund, dem in den USA 1200 Firmen, Universitäten und Institute angeschlossen sind – auch solche, die sich mit Rüstungsforschung befassen. Die angeschlossenen Firmen tätigen über Telenet Geschäfte oder tauschen Forschungsergebnisse aus.

Weil die Zahl der Benutzer so groß war, hielten die Hersteller den Code, der den Zugang zum Computernetz eröffnete, verhältnismäßig simpel. Im Falle von Telenet bestand der Code aus einer nur sechs- bis siebenstelligen Buchstaben- und Zahlenkette: Mit dem ersten Buchstaben wählt der Anrufer die Zahlungsart, mit der er später die Benutzungsrechnung begleichen will. Sodann folgt eine dreistellige Nummer, die mit der Telephon-Vorwahl des Distrikts identisch ist, in dem der angewählte Computer steht. Die letzten zwei bis drei Zahlen des Codes schließlich bahnen den Weg zu jeweils einem bestimmten Computer.

Die jugendlichen Elektronikspieler von Milwaukee tippten gewöhnlich die Vorwahl von Millionen-Städten ein, in denen besonders viele Computer stehen, etwa „213" für Los Angeles oder „212" für New York. Dann suchten sie durch Zufallskombinationen von zwei oder drei weiteren Ziffern an irgendeinen Computer heranzukommen. Gelang das, mußte allerdings noch ein Codewort eingetippt werden, um in das jeweilige Datensystem Einlaß zu finden.

Doch auch dieses letzte „Sesam, öffne dich!" verlangte den Teenagern keine sonderliche Phantasie ab. Zumeist waren es simple Codewörter wie „System", „Test" oder „Demo", Begriffe, wie sie häufig von den Computer-Firmen für ihre Wartungstechniker reserviert werden.

„Es ist gerade so, als ließe man in einem unverschlossenen Wagen den Schlüssel stecken", so charakterisierte Martin Hellman, Computer-Wissenschaftler der Stanford University und Regierungsberater für Datenschutz, das in vielen Fällen leichtfertige Sicherheitssystem von Computern – es sei geradezu „unmoralisch".

Nicht höher waren die Hürden für eine vierköpfige Teenagergruppe aus Irvine, Kalifornien, deren Heimcomputer bei der Großrazzia vom FBI gleichfalls beschlagnahmt wurden. Die Bundesbehörde hatte die verschiedenen Gruppen von Computer-Kids schon seit Juli im Visier gehabt: Seit Monaten trieben sich Jugendliche im Computer-Netz der US-Raumfahrtbehörde Nasa herum.

Daß „Hacker" wie die Gebrüder Greg und Gary Knutson, 14 und 15, oder deren Freunde große Teile des Nasa-Datenbestandes gleichsam per Fernbedienung gelöscht hätten, wurde inzwischen von einem Nasa-Sprecher dementiert: Die Fremdgänger hätten lediglich zum elektronischen internen Nachrichtenverkehr der Behörde Zugang gefunden.

Zumeist hatten die Jugendlichen, die auf dem Bildschirm mit „Mad Bomber" oder „S. Shuttle" unterzeichneten, verrückte Botschaften hineingefunkt, zum Beispiel den Weltkrieg-II-Slogan von US-Soldaten „Kilroy was here". Mitunter fanden Nasa-Angestellte einen geharnischten Brief von ihrem Abteilungsleiter auf dem Bildschirm; der seinerseits erhielt eine rotzige Antwort – beides hatten die „Hacker" frei erfunden.

Den geschickteren unter den Eindringlingen war es allerdings auch gelungen, sich im Nasa-Rechner eigene, verborgene Nischen einzurichten, von deren Existenz die Nasa-Leute keine Ahnung hatten; die Teenager nutzten die Nischen zu kostenlosem Nachrichtenverkehr quer durch die Vereinigten Staaten.

Auch in diesem Fall waren die Codes, die von den Jugendlichen geknackt werden mußten, denkbar einfach. Das Codewort für den Zugang zu dem Nasa-Computer bestand aus zwei Buchstabenkombinationen: Die Nasa-Angestellten mußten nur die Anfangsbuchstaben ihrer Vornamen und ihren Familiennamen eintasten – erste Abteilung. Der zweite Teil des Codes war, der Einfachheit halber, auf einen einzigen Buchstaben reduziert: A. Listen mit Namen und Vornamen aller Nasa-Angestellten sind gegen geringe Gebühr erhältlich.

Offenbar blieb der Computer-Spuk bei der Nasa noch relativ harmlos. In anderen Fällen richteten Hacker mehr Unheil an, so zum Beispiel bei einer Leasing-Gesellschaft in Los Angeles, wo letztes Jahr ein Teil der Daten zerstört, andere (so ein Firmensprecher) „mit Obszönitäten durchsetzt wurden". Geschätzter Schaden: 250 000 Dollar.

Vor allem von Banken, so erläuterte ein Experte, würden derartige Vorfälle häufig gar nicht erst gemeldet. „Sie ändern stillschweigend die Codewörter,

Ex-„Hacker" Sloane: Programme meistbietend verkauft

und man hört weiter nichts davon." Längst haben die Computer-Youngster die Datenschützer bei Banken und Großunternehmen das Fürchten gelehrt: Die „Whiz Kids" betreiben – natürlich über Bildschirm – einen florierenden Austausch von Informationen: „Biete Codewort zum Brookhaven National Laboratory, suche Schlüsselwort für anderen Großcomputer." – „Biete Zugangscode zum Dow-Jones-Börsencomputer – gegen Anleitung zu seiner Benutzung."

Die Info-Dienste arbeiten unter Decknamen wie „Piratenhöhle" und „Secret Service", ihre Benutzer tarnen sich mit Pseudonymen wie „Lord der Finsternis", „Mr. Schlüpfrig" und „Fliegender Korsar". Einer der Informationsdienste, ansässig in Boston, lieferte kürzlich eine komplette Liste der Zugangscodes von mehr als 200 Firmen-Computern, darunter von General Motors und der New Yorker Citibank.

Als intellektuelles Spiel, zur Schärfung des eigenen Computer-Verstandes, betrachten wohl die meisten „Hacker" ihr fragwürdiges Tun.

„Es ist eine Art Herausforderung, herauszufinden, ob man das Sicherheitssystem durchbrechen kann, das ein anderer ersonnen hat", so umschrieb es ein New Yorker Computer-Freak, der sich „Stainless Steal Rat" nennt. Manche auch sehen in den jugendlichen Pfiffikussen den brillanten Computer-Nachwuchs von morgen, verkörpert etwa in Burt Sloane, einem nun 20jährigen Ex-Hakker, der mittlerweile seine Programme meistbietend an Software-Firmen verkauft. Beispielsweise prüft er in deren Auftrag, ob ihre Programm- und Elektronikspiel-Kassetten hinlänglich gegen Raubkopierer gesichert sind.

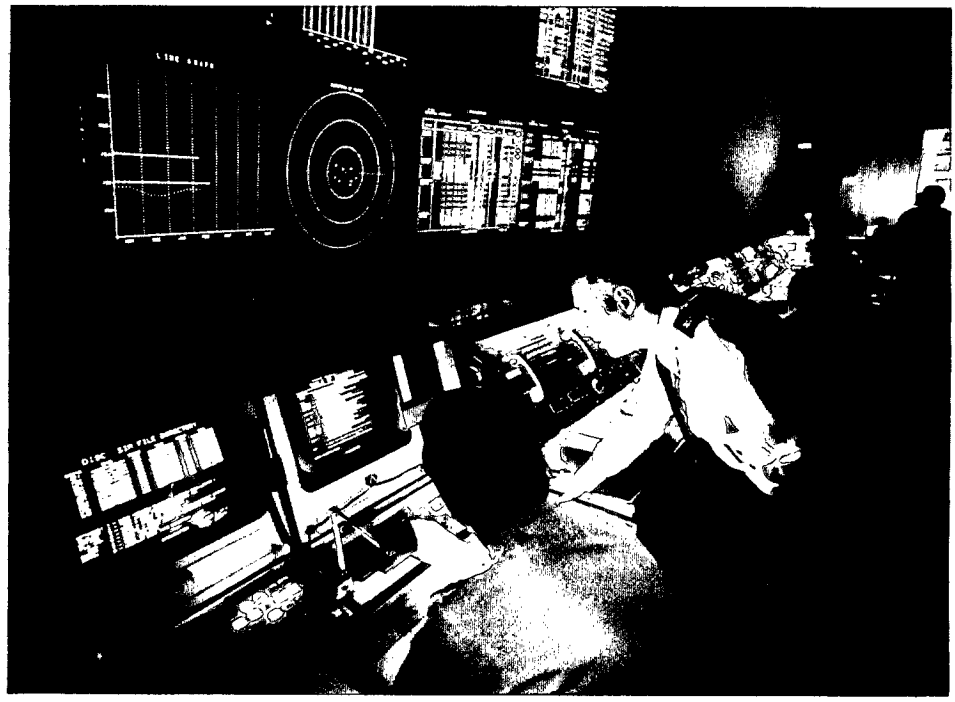
Doch die Amerikaner sind weit davon entfernt, die Computer-Spielerei noch länger zu verharmlosen. Schon als die „414er"-Gang aus Milwaukee aufflog, berichteten alle Medien in Schlagzeilen darüber. Das Nachrichtenmagazin „Newsweek" widmete den „Computer-Bubenstreichen" eine Titelgeschichte.

Denn längst ist deutlich, daß die Computer-Fummelei – außer daß sie wirtschaftlichen Schaden anrichtet – auch die höchsten nationalen Sicherheitsinteressen der USA berührt.

In dem Kino-Thriller „War Games", der vor kurzem in westdeutschen Filmtheatern anlief, wird gleichsam der elektronische „Super-Gau", der „größte anzunehmende Unfall", durchgespielt: Ein jugendlicher Computer-Fan verschafft sich Zugang zu den Rechnern der amerikanischen Atomkriegszentrale und löst, indem er an seinem Home-Computer herumfingert, beinahe den nuklearen Holocaust aus.

So schlimm, sagen Experten, könne es – zumindest auf absehbare Zeit – nicht kommen. Der Film sei reine Fiktion.

Die Rechner der amerikanischen Luftverteidigungszentrale „Norad" und des Strategischen Bomberkommandos



SAC-Kommandozentrale: Datenverkehr über „gehärtete" Leitungen

(SAC) der USA unterliegen seit Jahren der „Härtungs"-Kontrolle durch den Super-Geheimdienst, die National Security Agency (NSA): Nur ausgewählte Personen haben Zugriff zu den Rechnern. Die Rechnerräume sind so abgeschirmt, daß keine Spur von elektromagnetischer Strahlung, die sich anzapfen ließe, nach außen dringt. Datenströme die nach draußen gehen, werden nur über gesicherte Übertragungsleitungen geschickt und sind mit mathematischen Super-Codes verschlüsselt.

Doch derart gesichert sind nur die wichtigen Nervenzentralen des westlichen Verteidigungssystems. Insgesamt aber wird auch das militärische Computer-Netz immer verletzbarer, weil es in fast schon unüberschaubarer Breite um den Globus wächst. Zunehmend, so erläutern Pentagon-Experten, müßten auch streng geheime Nachrichten und Daten, etwa von Frühwarn-Satelliten oder vorgeschobenen elektronischen Horchposten, durch Rechnernetze rings um die Welt transportiert werden.

Mehr als 100 Millionen Dollar hat das US-Verteidigungsministerium schon in den vergangenen Jahren für zusätzliche Computer-Sicherheit aufgewendet. Hochqualifizierte Wissenschaftler wurden vom Pentagon beauftragt, Schwachstellen im Netz ausfindig zu machen, indem sie sich in die Rolle von Computer-Saboteuren hineindenken.

Und in der Tat: Immer wieder gelang es den Experten, auch in scheinbar perfekt abgeschirmte Systeme einzubrechen. „Immer aufs neue", so Pentagon-Sicherheitsberater Parker, „fanden sie neue Löcher in dem System, das ohnehin einem Schweizer Käse gleicht."

Noch unheimlicher als die Sorge um Übertragungswege ist den Pentagon-Experten der Gedanke an die immer komplexer werdenden Programme in den Rechnern des militärischen Apparats. „Je umfangreicher und komplizierter die Programme werden, um so leichter sind sie auszutricksen, lassen sich Fallen einbauen", erläuterte Louis W. Tordella, ehemals Abteilungsleiter bei der NSA.

Computer-Fachleute rechnen etwa mit der Möglichkeit, daß Agenten und Saboteure das militärische Computer-Netz der Amerikaner für ihre Zwecke umfunktionieren könnten, mit Programmen, die sie an allen Sicherheitskontrollen vorbei in das Netz einschleusen, ohne daß es irgend jemand bemerkt.

Solche „schlafenden Programme" würden erst durch bestimmte Signale, etwa die Alarmmeldung einer Radar-Frühwarnkette, aktiviert, um sodann tödliche Verwirrung in den Computern des Verteidigungssystems zu stiften.

In einem solchen „Meer von Gefahren" („New York Times") rudern die Daten-Sicherer des Pentagon einstweilen ziemlich hilflos. Allerdings gelang es ihnen sofort, bei der Reagan-Administration weitere Mittel lockerzumachen: Der Aufwand für das Computersicherheits-Zentrum beim Pentagon wird mehr als verdoppelt.

Als erste einschneidende Maßnahme wurde Anfang dieses Monats beschlossen, das seit 15 Jahren bestehende riesige Datenverbundnetz des Verteidigungsministeriums in zwei getrennte Systeme aufzuknacken.

Bisher hingen zahlreiche Rüstungsfirmen sowie eine Reihe von Universitätsinstituten, die für das Pentagon forschen, mit am Netz. Künftig sollen alle nichtmilitärischen Einrichtungen vom Pentagon-Computer abgekoppelt und zu einem eigenen Verbundnetz zusammengeschaltet werden. ◆