kehrter Richtung kann nicht manipuliert, sondern nur ein Dialog geführt werden. Für den Bedarfsfall im eigenen Bereich wird man, so stelle ich mir das vor, wohl nur umgekehrt installieren müssen.

Beim Service-PC wird „Carbon Copy +" mit „cchelp" (Enter) gestartet. Es erscheint ein Menü. U.a. wird die Belegung der Funktionstasten angezeigt. Hiervon interessiert zunächst F1. Um die Verbindung zum Anwender-PC aufzubauen, ist F1 zu drücken. Wenn eine Modemverbindung herzustellen ist, kann dann mit Hilfe der Cursortasten aus einer Ruf-Tafel ausgewählt und mit Enter gewählt werden. Anschließend ist, wenn nicht (wie hier) schon automatisch geschehen, das Paßwort einzugeben. Wie versprochen, erschien auf dem Service-PC-Bildschirm das gleiche Bild, das zur selben Zeit auf dem Bildschirm des Anwender-PC in der Kanzlei stand. Mit F10 wurde die Fernbedienung des PC möglich, der in der Kanzlei die /36 emulierte. So erfuhren wir schließlich aus der Buchhaltung den gesuchten Preis.

Mit F7 wird die Terminalemulation eingeschaltet. F7 arbeitet nur auf der CCHELP-, also Service-Seite. Die Terminalemulation ermöglicht - so das Handbuch - den Dialog mit der weiten „Computer-Welt". File-Transfer kann nach den Protokollen XMODEM und KERMIT übertragen. Mir gefällt, daß auch hier Script-Dateien erstellt und verwendet werden können. Sie sollen kompatibel mit Crosstalk sein. Leider scheinen sie mir nicht kompatibel zu Sidekick Plus. Darüber hinaus habe ich nicht entdecken können, daß es einen Lernmodus wie bei Sidekick Plus gäbe. Das Handbuch beschreibt jedoch recht ausführlich, wie man eine Script- Datei erstellt. Wer die Anleitung überhaupt liest, müßte sie auch in die Tat umsetzen können. Carbon Copy kann übrigens, wie Sidekick auch, speicherresident (ca. 145 KB) geladen werden. Wer weitere TSR-Programme verwendet, muß sich dann über die Startup- Tasten-Kombination Gedanken machen, damit auf die entsprechende Aktion auch die gewünschte Reaktion erfolgt. Ein weiterer - hier nicht weiter zu verfolgender -Problempunkt scheint mir die Reihenfolge, mit welcher die TSR-Programme zu laden sind, wenn sie sich nicht stören, sondern ergänzen sollen.

Der ferne PC ist ganz nah...

Wegen der Möglichkeit, am fernen PC so zu arbeiten, wie wenn er vor einem stünde, scheint mir Carbon Copy Plus ein äußerst reizvolles Programm. Als typische Beispiele für die Nutzung der Fernbedienungsmöglichkeit sind angegeben: Aufspüren von anfänglichen Bedienungsfehlern, Retten von defekten oder gelöschten Dateien, Übertragen von neuen Software-Updates. Bevor man einen Anwendungshinweis umständlich beschreibt, könnte man ihn gleich vor- und ausführen. Für denjenigen, der nicht andere unterstützen will oder muß, gibt es fast noch interessantere Möglichkeiten. Er hat vom fernen Einsätzort aus, z.B. mit Hilfe eines Laptop-Computers, vollen Zugriff auf die heimatliche EDV. Diese hat vielleicht den größeren und aktuelleren Speicher. Sind die Daten zu Hause nicht mehr aktuell, können sie ferngesteuert aktualisiert werden. Im geschilderten Anwendungsfall konnte eine nicht oder nicht ohne weiteres fernbedienbare Anlage auf dem Umweg über PCs und Carbon Copy fernbedient werden.

Ungeklärt mußte ich lassen, ob Carbon Copy über Akustikkoppler eingesetzt werden kann. Im Handbuch habe ich mich vergeblich nach Hinweisen umgeschaut. Probieren konnte ich nicht.

Meine persönliche Kosten - Nutzen - Analyse ergab, daß ich mit Sidekick Plus auskommen werde. Ca. 450-700 DM (je nach Bezugsquelle) pro Version von Carbon Copy Plus wären für meine aktuellen Bedürfnisse eine übertriebene Ausgabe.

In Heft 16 der DFN-Mitteilungen (DFN = Deutsches Forschungsnetz) hat Herr Bauerfeld, Mitarbeiter des DFN-Vereins, einen sehr lesenswerten Beitrag zu der die (auch juristische) Öffentlichkeit immer stärker beschäftigenden Frage des „Hacking" geschrieben. Wir freuen uns, daß der DFN-Verein uns die Übernahme dieses Beitrags gestattet hat. Die Überlegungen von Herrn Bauerfeld ergänzen in passender Weise den Beitrag in diesem Heft, der sich mit der Frage der Strafbarkeit des „Hacking" befaßt. Zu dem Nachdruck haben wir uns auch deswegen entschlossen, weil die DFN-Mitteilungen (sehr zu Unrecht) unter Juristen noch nicht die Resonanz gefunden haben, die sie verdienen. Vielleicht ändert sich das in naher Zukunft, wenn die neue Benutzergruppe der mit Rechtsinformatik befaßten juristischen Hochschullehrer im DFN ihre Tätigkeit aufgenommen hat. (Jur-PC wird regelmäßig darüber berichten:)

Hier wird gehackt

Dr. Wulfdieter Bauerfeld*

Oswin K. legt die „Bayerische Hackerpost *** Das Informationsblatt für den lebensbejahenden DFÜ-Benutzer" beiseite und schiebt eine Diskette in seinen mit dem Telefon verbundenen Home Computer. Der Anschluß ist so „erweitert", daß Oswin K. das Erzeugen der Wählimpulse dem Programm „Sherlock" überlassen kann. Es wählt in einem vorgegebenen Bereich jeden Teilnehmer an und überprüft, ob vom anderen Ende ein hoher Ton - die Trägerfrequenz eines potentiellen Kommunikations-„Partners" - ausgesendet wird. Diese Nummern werden gespeichert, anderenfalls innerhalb von 3 Sekunden „aufgelegt". Morgen will sich Oswin K. mit den „heißen" Telefonnummern näher befassen, vielleicht ist das eine oder andere interessante Zielsystem dahinter angeschlossen.

Ewald W. ist Sysop, er betreibt als System-Operateur auf einem leistungsfähigen Personal Computer ein Mailbox-System.

Von außen kommende „Mehlboxer" hinterlegen und finden mit Decknamen wie „Zombi", „Erpel", oder „producer" versehene Mitteilungen auf ihren als Schwarzes Brett fungierenden Bildschirmen: „Kermit: Sources für Dutzende von Rechner zum Tausch", „500 NUA's aus dem In- und Ausland". Es werden z. B. weltanschauliche Thesen an die programmierten Pinboards geschlagen, die in ihrer Brisanz, der Aktualität und

Dr. Wulfdieter Bauerfeld ist Mitarbeiter beim DFN-Verein, Zentrale Projektleitung, Berlin

ch die Dialogfähigkeit -Gegenthesen können daneben „ge-
ıgt" werden" - eine Leserbriefseite zu einem langweilig,
rren Forum werden Gabriele T. ist als eine der noch immer
lten zu findenden Frauen in der Szene umworbene Kundin
ei vielen Sysops. Außerdem hat sie Zugang zu einem PAD, so
aß ihr über DATEX-P auch Verbindungen ins Ausland mög-
ich sind. Regelmäßig hängt sie sich bei Delphi in den USA ein
und ruft dort Informationen zu Wissenschaft, Politik, Medizin
und Literatur ab.

So sehen Momentaufnahmen einer Subkultur aus, deren Protagonisten unter dem Stichwort „Hacker" durch die etablierten Medien geistern: „Computer-Freaks, die nächtelang auf der Tastatur eines Computers herumhacken, in der Hoffnung, in einem fremden System zu landen: in Computer-Programmen von Universitäten, Banken oder Konzernen". Sie suchen dasAbenteuer als in Computernetzen herumschweifende Datenrebellen, verspüren als Mitglieder einer „Paßwort-Knacker-Bande" berauschende Kitzel, wenn sich auf ihren Bildschirmen mit „Connected to the NASA Control Center/Houston, Please Login" ein System zum „Einbruch" anbietet. Für den Normalbürger, arbeiten Hacker kriminell oder zumindest hart am Rande der Legalität. „Hacking", sagt dagegen Wau Holland vom Hamburger Chaos-Computer-Club, „ist mehr als das Eindringen in ein technisches System. Es ist eine Denkweise".

What is a „hack"?

Einen „Hack" haben amerikanische Studenten zunächst eine besonders gelungene Problemlösung, später einen Streich getauft, mit dem Technik intelligent ausgetrickst wird. Dabei soll einer ungeschriebenen Ethik folgend niemandem körperlicher Schaden zugefügt werden; Hacking kann sich aber gegen anonymisierbare Einrichtungen richten, die im weitesten Sinne zur Versorgung dienen bzw. allgemeine Dienstleistungen anbieten.

Folgerichtig gab die seit fünfzehn Jahren erscheinende Zeitung „Technological American Party - TAP" (to tap = anzapfen), der schon legendäre „Hobbyst's NewsletterfortheCommunication Revolution" Tips, wie „Phone Phreaks" umsonst oder für wenig Geld über öffentliche Einrichtungen kommunizieren können: Mit einer kleinen elektronischen Schaltung, genannt „Black Box" telefoniert man gratis, weil es beim Angerufenen immer nur zu klingeln scheint („hochohmig rangehen, anstatt abzuheben"); mit der Blue-Box werden Gratisanrufe gemacht, weil sie die gleichen Signaltöne wie der Operator erzeugt, und mit der Red-Box lassen sich die in den USA für den mithörenden Operateur wichtigen Münzeinwurfgeräusche simulieren. Ähnliche Hacks gab es früher auch im Telefonnetz unserer Bundespost.

Hacking als Gemisch von jugendlicher Frechheit und technischem Sachverstand vermag eine Gefühlswelt zu öffnen, der ein wirtschaftlicher Vorteil zunächst nachgeordnet scheint. Gelingt ein Schlag gegen ein technisches System, dann wird er als Befreiungsschlag angesehen, der mit dem Apparat den Triumph über die Apparate ermöglicht.

Ist Hacking strafbar?

Zu häufig ausgeteilte Schläge verursachen empfindliche Schäden. AT&T, die amerikanische Telefongesellschaft, beklagte ei-

Besuche bei Hacker Helmut

Hacker Helmut wählt die Telefonnummer 24 00 01. Ein leises Pfeifen ertönt; die Verbindung mit dem PAD der Deutschen Bundespost in Berlin ist hergestellt. Hacker Helmut legt den Telefonhörer auf den Akustikkoppler und gibt am PC einen Punkt als amtsdeutsches „Dienstanforderungssignal" ein. Der PAD meldet sich am Bildschirm und bittet den Terminalnutzer, sich für diesen Postdienst zu identifizieren: Es wird die NUI (Network User Identification) erwartet, anhand der die anfallenden DATEX-P-Kosten abgerechnet werden und ein zusätzliches Paßwort.

Hack 1:
Der Hacker benutzt nicht seine eigenen NUI (falls vorhanden), sondern die von Werner K. (samt Paßwort). Werner K. arbeitet beim Softwarehaus „Comm-Mit" und hatte bei einer Vorführung auf der letzten Messe:... Besucher unvorsichtigerweise über seine Schulter gucken lassen/ NUI und Paßwort auf dem Terminal mit einer „Funktionstaste" fest eingespeichert, so daß auch andere die Informationen auslesen konnten/alle Angaben auf einem Zettel liegen lassen.
Es wäre aber auch gegangen mit Hilfe (des legalen)

Hack 2:
Der Hacker benutzt keine NUI, sondern gibt am Terminal für den PAD nur den Buchstaben,R, gefolgt von einer NUA ein.
Diese Zeichenkombination kann Hakker Helmut auch per Programm absenden. Über das Telefonnetz gibt er NUA,sweiter und läßt den PAD über DATEX-P beliebige Endteilnehmer anwählen, meist mit dem Ergebnis „call cleared - not in service". Wenn nun innerhalb einer Minute keine Verbindung zustande kommt, unterbricht der PAD mit einer Fehlermeldung die Verbindung zum Terminal. Dann sind wieder 23 Pfennig fällig, um erneut den PAD anzuwählen und mit,R, in den" („Probieroffiziell „Reverse-Charging-") Modus zu gelangen; doch ein Hacker und sein Programm kennen:

Hack 3:
Kurz vor Ablauf einer Minute, unterbricht der PC das Probieren und wählt die NUA eines bekannten Endsystems an, das „Reverse Charging" zuläßt. Dort meldet sich das Rechensystem der Fa. „Hosenmatz", die Bestellungen auch über Datenfernübertragung entgegennimmt, aber ihre Kunden nicht mit DATEX-P-Kosten belasten will. Solche NUA's werden „Park-Adressen" genannt und erhält man: ... beim Clubabend/aus der Hackerpost/ durch Zufall.
Da nun eine Verbindung hergestellt worden war, ist der Post-PAD beruhigt. Das Programm läßt diese als uninteressant wieder abbrechen und probiert bis zu einem Erfol oder für 58 Sekunden neue NUA's. Bei Erfolg melden sic Rechner, manche einsilbig („HK V3. 1"), manche höflic „Connected to THE SOURCE, please type ID, followed your number" (NUA 0311030100038).

Hack 4:
Private PAD's - kleine Rechenanlagen - verbinden vor ein oder mehrere Terminals oder Rechensysteme als Art Nebenstellenanlage mit DATEX-P. Während es Telefon nicht möglich ist, sich in eine Untervermit einzuwählen und sich ohne Angabe einer Nebenstell der über eine Amtsleitung hinauszuwählen, geht e (noch): Ohne ein Endgerät anzusprechen, lasser PAD's zu, über ein Kommando gleich wieder einen Ausgangskanal, z. B. für Auslandsverbindungen, zu

nen Verlust von 25 Millionen Dollar jährlich durch „Phone Phreaks", genug Geld, um nicht wenigstens einen Teil einklagen zu wollen. Da ein Hacker aber keine „fremde bewegliche Sache" in der Absicht wegnimmt, sich dieselbe „rechtswidrig zuzueignen" (Diebstahl, § 242 Strafgesetzbuch) oder eine andere Person in „Bereicherungsabsicht täuscht" (Betrug, § 263 Strafgesetzbuch), kam und kommt es bei vielen Hacks zwar zur Anklage, aber dann zu einem „Freispruch mangels Tatbestandes". Dem folgten und folgen immer wieder juristische Grundsatzdiskussionen: Ist Strom eine „Sache" - ein Ergänzungsparagraph (248c) stellt inzwischen die „Entziehung elektrischer Energie" unter Strafe; da ein Automat nicht betrogen werden kann, regelt als Zusatz §265a das Erschleichen von Leistungen. So bilden Hacks Modellfälle, an denen sich die Evolution unseres juristischen Systems messen muß, um mit dem sich durch technische Systeme notwendigerweise ändernden Weltbild mithalten zu können. §248b regelt den unbefugten Gebrauch eines Fahrzeuges gegen den Willen des Berechtigten, einen derartigen Paragraphen für den unbefugten Gebrauch von Rechenzeit Was ist dann aber mit unseren oben vorgestellten Hackern? Kriminell im Sinne von eklatanten Gesetzesverstößen ist keiner dieser so geheimnisvoll agierenden Personen. Zugegeben, Oswin hat postalische Bestimmungen verletzt, als er den Telefonapparat (Eigentum der Bundespost) durch eine nicht zugelassene automatische Wähleinrichtung erweiterte. Ewald baut zur Zeit ein sogenanntes Modem, was zwar billiger, aber damit nicht postzugelassen sein wird. Und Gabriele hat ganz offiziell einen Zugangscode zur Datenbank „Official Airline Guide" und kann so erfahren, daß Aeroflot wöchentlich zweimal von Omsk nach Tomsk fliegt. Die Kommunikationsmöglichkeit mit der Delphi-Box hat 200 DM Einmalgebühr gekostet und deren Inhalt ist für sie als Wissenschaftsjournalistin nicht nur von privatem Interesse.

Vom „Eindringen" in Netze

Offene Kommunikation kann und darf im wahrsten Sinne des Wortes kein Geheimnis sein. Und damit wird das Dilemma der Datenkommunikation sichtbar: Denn was dem Wissenschaftler oder dem kommerziellen Anwender recht ist, ist dem Hacker billig.

Was lehren uns die Besuche bei Hacker Helmut (s. Kasten)? Sind wir Lücken in der Gesetzgebung, dem fehlenden Fernmeldegeheimnis in der Datenkommunikation und groben technischen Unzulänglichkeiten auf der Spur? Wichtig ist zunächst, daß unsere Hacks ausschließlich auf das Betriebsmittel, Netz, und nicht auf die daran angeschlossenen Endsysteme konzentriert waren. Es wird die Nutzung einer öffentlichen Infrastruktur vorgeführt, die auf Kosten anderer mißbraucht werden kann. Das kennen wir aber bereits vom Telefon: Bei alten, auf Relaistechnik beruhenden Nebenstellenanlagen gab es einen bestimmten Wählkniff, der an vielen Universitäten über Studenten-Generationen hinweg vererbt wurde und „Gratis"-Ferngespräche erlaubte. „Hacks" bleiben in Datennetzen auch immer dann möglich, wenn bestimmte Informationen wie unterschriebene Blankoschecks herumliegen oder technische Sicherungsmöglichkeiten nicht genutzt werden.

Somit rückt das berüchtigte „Eindringen in Computer-Netze" in die Nähe eines ganz normalen Vorgangs. Es ist unnötig und technisch unsinnig, das) (DATEX-P-Kind mit dem (Hacker-) Bad auszuschütten. Wie die Anwahl eines bekannten oder unbekannten Teilnehmers im Telefonnetz niemandem verwehrt wird, mögen auch anonyme oder belästigende Anrufer die Möglichkeit haben, das Netz für ihre, eher unfeinen Ziele zu nutzen, sollten über Datennetze mit derselben Selbstverständlichkeit Kommunikation mit Rechensystemen möglich sein. Die Gefahr, technisch sinnvolle, verteilte Projekte die auf solche Kommunikationsmöglichkeiten angewiesen Wie sieht es aus mit dem „Herumwandern" in Datennetzen? Auch Hackern sind nur bestimmte Dienste zugänglich, hinter denen sich ganz reale Kabel verbergen. Falls nicht durch posteigene Brücken vorgesehen, läßt sich ohne Erdarbeiten oder technische Manipulationen an posteigenen Einrichtungen eine Kommunikation zwischen untererreichen. Die Senatsdienststellen von Hamburg und Berlin, die Bundesbahn, die Elektrischen Versorgungsunternehmen betreiben seit Jahren private Kommunikationsnetze, ohne daß sich bisher ein Haker brüsten konnte, dort illegal herumgewandert zu sein. Und über öffentlichen Datennetze ist - ähnlich wie über öffentliche Telefonnetze - das Übermitteln sicherheitsrelevanter Informationen nicht geraten.

Darüber hinaus ist das „Abhören" von u. U. codierungsgesicherten Kommunikationsverbindungen mit einem erheblichen technischen Aufwand verbunden, der eine unverhältnismäßig komplizierte Ausstattung an Betriebsmitteln und Know-how erfordert. Die Lufthansa, Banken oder die untereinander verbundenen Rechensysteme der Landesverwaltung von Nordrhein-Westfalen nutzen teilweise öffentliche Kommunikationsdienste (DATEX-L bzw. DATEX-P), wohlwissend daß niemand die Informationen der zwischen den Systemen wandernden Daten ergründen wird.

Das jedes technische System mit einem entsprechenden Aufwand „geknackt" werden kann, kann nicht abgestritten werden. Insbesondere sind bei Kommunikationseinrichtungen in privater Hand (siehe PAD) erhebliche Mängel festzustellen. Ein potentielle Gefahr bei der Ausweitung von öffentlicher Rechnerkommunikation und der damit verbundenen Umorganisation von Kommunikationsstrukturen wird aber eher darinliegen, daß nicht Privatleute, sondern wohlorganisierte auch staatliche Stellen, unautorisiert oder auf der legalen Basis verschiedener Gesetze, sich Möglichkeiten verschaffen, um zum Wohle des Volkes „Gefahr im Verzuge" abwenden zu können.

Eine absichtlich oder zufällig gewählte Telefonverbindung bietet noch keine Gewähr für eine folgende, wenn möglich lange oder tiefgehende Unterhaltung. Am anderen Ende sind Menschen, für die bestimmte Verabredungen gelten, deren „Zugangscode" nicht jeder kennt. Nach einer Ablehnung kann man aber wieder versuchen, die Verbindung zum Partner zu knüpfen und wendet damit die klassische Hacker-Methode an: „Trial and Error". Hartnäckig untersuchen sie eine Möglichkeit nach der anderen, um über Datennetze mit den Endsystemen, den Rechner ins „Gespräch" zu kommen. Hier geht es also nicht um das illegale Nutzen von Kommunikationseinrichtungen wie Datennetzen, sondern endlich um das „Eindringen in ein Endsystem". Mit einem Klein-Computer als Grundauastattung lassen sich Bedienungsabläufe der Nutzer-Schnittstellen beliebig oft wiederholen und bestimmte Kombinationen ermüdungsfrei ausprobieren. Und damit sind wir wieder beim Bild von den „Computer-Freaks, die nächtelang auf der Tastatur eines Computer herumhacken - in der Hoffnung in einem fremden System zu landen".

System-Knacker

Durch die Möglichkeiten des vielfach über DATEX-P zusammengeschlossenen Deutschen Forschungsnetzes hat die Wissenschaft mit ihren vielfältigen und ständig wachsenden Kommunikationsbeziehungen eine Vorreiterrolle, um Rechnerkommunikation über öffentliche Datennetze zu demonstrieren. Sie mußte in den ersten Jahren aus unangenehmen Erfahrungen lernen, mit den neuen Möglichkeiten operativ umzugehen. Beobachten wir einen Hacker, der versucht, z. B. in den Großrechner einer wissenschaftlichen Einrichtung einzudringen. Zum „Landen" im Betriebssystem ist Kenntnis einer Nutzerkennung und eines Paßwortes notwendig. Kennungen lassen sich oft bei Kenntnis des Betriebssystems und der angewählten Institution erraten. Ziel ist ein VAX-Rechner im Institut für Astrophysik. Vermutlich fangen dort alle Kennungen mit !AP an. Nach dem erfolgten Verbindungsaufbau über DATEX-P bietet der Hacker dem Betriebssystem die Kennung !AP275 an, vom System erscheint als Antwort „Paßwort".

Nun kann ein „Scan-Programm" angesetzt werden, welches Buchstabenkombinationen als mögliche Paßwörter erzeugt und dem Rechner anbietet. Für ein Paßwort von n Zeichen (26 Buchstaben und 10 Ziffern sind zugelassen) sind damit 36**n Kombinationen möglich. Das bedeutet bei vier Zeichen zwar „nur" 1 67961 6 Versuche, aber... Paßwörter haben oft mehr als nur vier Buchstaben und viele Betriebssysteme unterbrechen die DATEX-P-Verbindung, wenn nach einigen Versuchen immer noch kein ordnungsgemäßes Login stattgefunden hat. Das bedeutet dann selbst bei einem schnellen und willigen PC eine ganze Menge Zeit und - drum nutzt man nie die eigene NUI! -Verbindungsaufbaugebühren.

Mit dem Programm HANS - Hacker Network Service - arbeitet der Hacker wie mit einem umgebogenen Draht am Türschloß: einfach, unkompliziert und schnell. Dann nämlich, wenn der Benutzer, den der Hacker vorgibt zu sein, das Standard-Paßwort, welches beim Generieren des Betriebssystems für alle automatisch eingerichtet worden war, noch nicht verändert hat. HANS hat eine ganze Reihe solcher Standard-Paßwörter gespeichert, für manche Betriebssysteme sind es bestimmte Zwei-Zeichen-, bei anderen gleichlautende Vier-Buchstaben-Kombinationen.

Aber nicht alle Benutzer einer Rechenanlage lassen zum Schutz des Zugangs nur das Schnappschloß an ihrer Eingangstür zufallen. Bei hartnäckigeren Fällen ist beim Hacker und seinem Helfer HANS Esprit und angewandte Psychologie gefragt. Wird sich ein „normaler" Benutzer eines im DFN verfügbaren Rechners zu DFNETZ 002645 als Paßwort ein umständliches „03JX1 0F37" aussuchen? Ein zur Kennung gleichlautendes Paßwort kann er sicher leichter memorieren.

Nicht aufgeben, wenn auch das nicht stimmt. Wahrscheinlich kann sich dann unser fiktiver Nutzer am leichtesten an den Namen seines Lebenspartners erinnern. Und da ein Gutteil der naturwissenschaftlichen Rechnernutzer Männer sind... hält der gute HANS auch einen Katalog von bis zu 2000 Mädchennamen auf dem PC bereit, die nacheinander ausprobiert werden können.

Ein alter Informatikerwitz lautet „Mein Paßwort ist geheim". Oft ist das wörtlich zu nehmen, auch Unmengen von „Gandalfs", „Merlins" und anderen Zauberergrößen gehören zu Lieblings-Paßwörtern, die zwar über komplexe Zugriffsmechanismen geschützte Dateien der Hostrechner gespeichert und damit selbst für den Rechenzentrumsverwalter unerreichbar, aber eben leicht zu erraten sind.

Juli 1984: Die Deutsche Bundespost geht mit ihrem Teleboxsystem an einem Host in Mannheim (NUA 45621 040000) in den öffentlichen Probebetrieb. Eine Liste der Erst-Abonnenten für dieses Mailbox-System ist erhältlich.

Eine am Probebetrieb beteiligte Firma wählte ein zum Firmennamen hervorragend passendes Codewort. Ein Hacker fand diese Kombination offenbar ebenfalls sehr zutreffend, denn nach wenigen Versuchen meldete sich der Rechner in Mannheim: „Willkommen im Telebox-System! Ein Menü in INFO-Dateien erhalten Sie mit dem Befehl INFO INFO". Man war „drin"...

Als Folge findet am 13. Juli 1984 jeder Telebox-Kunde in seinem elektronischen Briefkasten einen Rundbrief von FTZ007, der Kennung des Betreibers:
„Betreff: Unberechtigte Zugriffe

Sehr geehrte Probeteilnehmer von Telebox, leider können wir bei der Einführung der Dienstleistung Telebox nicht immer davon ausgehen, daß das System nur in der vorhergesehenen Weise benutzt wird. Das Erschleichen von Leistungen wird mancherorts als Sport angesehen, obwohl es ein strafrechtlicher Tatbestand ist. Wir weisen noch einmal darauf hin, daß die Vertraulichkeit des Paßwortes vom Teilnehmer selbst sicherzustellen ist..."

Eine Bitte, an die sich jeder Benutzer oder Systemverwalter einer Rechenanlage halten sollte, mit der zusätzlichen Aufforderung in „Time-Sharing-Systemen" anstelle einfacher Schnappschlösser mindestens ein kompliziertes Sicherheitsschloß einzubauen. In ungeschützten Rechnern werden wir sonst weiterhin zu oft Spuren der Hacker finden, die wie den Graffiti auf der Hauswand ihr „Killroy was here" oder „Computer-Viren" hinterlassen haben.

Hacker als Stars?

„Größter Spionage-Fall seit Guilleaume" - eine Schlagzeile vom Februar dieses Jahres:

Was ist so sensationell an dem KGB-Spionagefall, der jetzt bekannt wurde? Die Tatsache, daß sich Geheimdienste immer der neuesten technischen Mittel bedienen ist genausowenig neu wie das Faktum, daß sich abenteuerlustige Halbwüchsige zu Taten hinreißen lassen, die sie später wieder bedauern. Für viele Kritiker stellen Rechenanlagen etwas grundsätzlich Neues dar. Mit ihnen sind zum ersten Mal Maschinen entstanden, die dem Menschen nicht Muskel-, sondern Kopfarbeit abnehmen. Der Nordamerikaner Josef Weizenbaum, einer der wenigen Mahner, sagt: „Computer sind erfunden worden, um die bestehenden Herrschaftsverhältnisse zu sichern".

Vielleicht möchte man den Hackern sogar die gesellschaftliche Vorreiterrolle (welcher Hacker wird das nicht gerne hören) zubilligen, uns auf die möglichen Gefahren völlig neuen Technologien aufmerksam zu machen. Bei den Betreibern des Herrschaftsinstruments Computer sind Hacker nicht nur unbe-

liebt, sondern werden in die Nähe von Saboteuren und Chaoten gerückt, allzu typisch für eine leichtfertige Kritik. „Hacken ist eine Denkweise", eine Denkweise, die in ihren Erkenntnissen schon weiter ist?

Doch Antworten von Hackern auf vielfältige Fragen in dieser Richtung sind eher ernüchternd oder bleiben ganz aus. Daß zur Schaffung moderner Kommunikationssysteme bestehende Netze miteinander verbunden werden müssen, wird begeistert ausgenutzt und technisch diskutiert, die möglichen sozial einschneidenden Folgen werden nicht begriffen.

Hacker, im wahrsten Sinne auch der deutschen Bezeichnung, führen sich als kleine Herren auf und überlassen den stupiden Teil ihrer „Arbeit" gerade dem Herrschaftsinstrument Computer, um sich so Leistungen zu erschleichen (Netzwerk) oder den Eingang in Endsysteme zu finden.

Die mangelnde Auseinandersetzung der Hacker mit den Gefahren der Datentechnik und Kommunikation mag aber ihre Ursache auch in einem bereits schieflastigen Ausgangspunkt haben. Wir suchen dann vergeblich bei den Hackern Kritik an einer gesellschaftlichen Bürde, die sie gar nicht tragen wollen oder können. Nur aus unserer arbeitsteiligen Welt heraus sind wir gewohnt, zwischen Hand- und Kopfarbeit zu unterscheiden, bauen aber daraus allgemeingültige gesellschaftliche Modelle. Viele Kritiker erliegen wohl zu sehr dieser Teilungsarroganz, wenn sie dann mit einem Male ernüchternd etwas qualitativ Neues an Maschinen entdecken, die uns keine Muskelarbeit und zum ersten Mal Kopfarbeit abnehmen.

Akzeptiert man die Fähigkeit des mechanistischen Weltbildes, Arbeit in vielfältiger Weise auf Maschinen zu übertragen, dann sind Hacker ebenfalls und als geradezu notwendig zu akzeptieren. Durch die „Veröffentlichung" von technischen Systemen wird frühzeitig ihnen und damit späteren Nutzern die Möglichkeit geboten, diese auszutesten und Entwurfsschwächen aufzudecken. Dies ist wie der Probelauf einer neuen Maschine ein lebendiger und wichtiger Teil des Systementwurfs, der gerade beim Aufbau einer offenen und öffentlichen Kommunikationsinfrastruktur zum Zusammenschluß von Rechensystemen notwendig ist und möglicherweise später wirklich entstehenden Schaden schon im Ansatz zu begrenzen hilft. Der etablierte, gesellschaftliche Wert eines „Test-Ingenieurs" mag dann manchen „bekehrten" Hacker auch verführen, mit der Industrie zu kokettieren.

Was bleibt da übrig von der Denkweise und dem gesellschaftlichen Glanz, ein Hacker zu sein: Immer noch genug, nämlich ein bißchen Vorbild darzustellen für die Aufgabe, sich frühzeitig mit Möglichkeiten und Folgen der offenen Kommunikation auseinanderzusetzen und jenen auf die Finger zu schauen, die nicht die totale Kontrolle über den Computer, sondern eine mögliche Kontrolle über den Bürger erreichen wollen. Und es bleibt übrig das scheinbare Erstaunen von würdigen „Abwehrern" über die Möglichkeit, sich in militärischen Rechenanlagen umzuschauen oder Programme bzw. Daten zu kopieren und damit zu „klauen". Entweder glauben viele Betreiber von Rechenanlagen immer noch nicht, daß es außerhalb ihres überblickbaren Machtbereichs Experten im Schulkinderalter gibt, oder sie wissen nicht, daß man auch „immaterielle Informationen" vor unautorisiertem Zugriff schützen muß.

Was tun?

Betreiber und Nutzer der an Datennetze angeschlossenen Systeme müssen sich bewußt werden, das anders als bei der physischen Anwesenheit eines Fremden in einem Büro, die „Anwesenheit" eines Eindringlings in einem Rechner viel leichter unbemerkt bleibt. Ein erfahrener Hacker wird sich zunächst wie ein normaler Nutzer verhalten, Dateien schreiben, lesen und löschen; einen eingedrungenen Hacker auf frischer Tat zu ertappen ist fast unmöglich. So müssen Sicherungen bereits an der Eingangstür eingebaut werden:

Zusätzliche Paßwörter für einen Netzzugang, Identifizierung anhand geheimer Nummernfolgen, diese können „altern" und damit ungültig werden. Eindringversuche ließen sich protokollieren und zurückverfolgen (der Nutzer des DATEX-P gibt, technisch bedingt, seine eigene NUA im ersten Datenpaket an) bzw. bestimmte Funktionen des Rechensystems für Außenstehende sperren.

Solche Hemmschwellen, eine verbesserte Organisation im Rechenbetrieb, und die Entwicklung von Betriebssystemen bzw. Programmen, die diese zusätzlichen Sicherungsmöglichkeiten bieten, sollten ein normaler Teil unseres Umgangs mit öffentlich zugänglichen Rechenanlagen werden.

Der neue „verteilte" Dienst, das von der CCITT empfohlene „Message Handling System X.400", bietet für viele über DATEX-P angeschlossene Rechner eine neue, sichere Zugangsmöglichkeit. Hier haben Systemfremde nur noch die Möglichkeit, einen Brief an die elektronischen Postkästen des Zielsystems zu versenden. Das Austragen der Briefe über DATEX-P an die einzelnen Zielsysteme übernehmen dabei „Message Transfer Agenten", Programme in Knotenrechnern, auf die ein Nutzer keinen direkten Zugriff mehr hat. Die vielfältigen Möglichkeiten des „sicherheitsgefährdenden" Dialogs können so potentiellen Hackern versperrt werden, ohne daß auf eine nutzerfreundliche elekronische Kommunikation verzichtet werden muß. Andere Systeme haben sich auch auf die „Neue Öffentlichkeit" bereits eingestellt und bieten spezialisierte Dienste an, so ECHO (NUA 02704481 1 2) „a really public host in Europe". Das Angebot umfaßt Informationsdateien über DIANE (Datenbanken, Anbieter und Zielrechner in Europa/Paßwort für die deutsche Version DIANED), Ausschreibungen an europäischen Projekten (CALLID) oder die neuesten Wechselkurse für die europäische Währungseinheit ECU (ECU). Und falls mehr Informationen über DFN gewünscht werden, eine Datenbank steht über DATEX-P (NUA 45300043042) zurVerfügung. Das Zielsystem verrät sogar den öffentlichen „Login-Namen" (dfn) und das Paßwort (infosys). „Loggen" Sie sich doch einfach mal ein!