Löcher im Netz – Datensicherheit bei Bildschirmtext

„Manipulationstechniken der Computer-Kriminalität" lautete das Thema eines Fachsymposiums, veranstaltet vom Leuro-Seminar München. Prominentester Gastredner war Richard Cheshire, ungekröntes Haupt der datenbankknackenden Computerkinder Amerikas. Den deutschen Btx-Teilnehmern prophezeite er düstere Zeiten.
OP-Autor Dipl.-Ing. Roland Dreyer fand auf die Frage „Wie sicher ist Btx?" erstaunliche Antworten.

„Die Hacker wollen ihren Titel wiederhaben" forderte Cheshire Catalyst alias Richard Cheshire. Spätestens seit seinem Interview im ‚Spiegel' kennt man auch bei uns den Hackerkönig und Herausgeber des amerikanischen Underground-Blättchens „TAP". „TAP" ist beliebt, gibt es doch Hinweise, wie man kostenlos Ferngespräche führt, Datenbanken anzapft und Verwirrung in Mailboxen, den elektronischen Briefkästen, stiftet. Der Titel steht für „Technological Assistance Program"; daß „to tap" auch anzapfen, abhören heißt, stört die meist jugendlichen Leser wenig.

„Hacker sind", meinte Cheshire leutselig, „nur phantasievolle Kinder, die solange auf der Tastatur ihres Home-Computers herumhacken, bis sie all' seine Möglichkeiten ausgeschöpft haben". Gelingt ihnen die Datenverbindung via Telefon mit einem kommerziellen Rechenzentrum, ist es für sie ein Heidenspaß, dem verdutzten Operator einen munteren Spruch auf seinem Sichtgerät zu präsentieren. Böses liegt ihnen fern, und sie begreifen gar nicht, warum der FBI immer entschlossener Jagd auf sie macht. Denn mit den „Crackern", den wirklichen Byte-Banditen, haben sie nichts zu tun. Das sind die Bösen, die Informationen und Programme stehlen, um sie gegen harte Dollars zu versilbern. Manchmal lassen Sie sich das Geld auch gleich aufs eigene Konto überweisen, das sie mit einem erschlichenen Paßwort ihrem Nachbarn vom Bankkonto filzen. Richtig teuer wird es aber erst, wenn Cracker Industriespionage machen – natürlich ohne daß es einer merkt.

Dr. Jay Bloom-Becker, Direktor des National Center for Computer Crime Data, Los Angeles, will mit derlei feinsinniger Unterscheidung gar nicht erst anfangen. „Verdorbene Kinder, ohne ein Gefühl für Verantwortung und Eigentum" schalt er die computerisierten Hackerbuben seiner Heimat. Und sein Tischnachbar Cheshire sei schließlich einer, der in „TAP" zu kriminellen Handlungen aufrufe.

Der junge Vollbart trug's mit Fassung. Er weiß: im Grunde sind ihm alle Beteiligten – Rechenzentren, Polizei und Datenschützer – dankbar, daß er so schmerzhaft den Hackerfinger auf eine seit langem offene Wunde legt. Zeigt doch seine Gemeinde den EDV-Experten, daß sie ihr Paradies der sicheren Computer längst verloren haben.

Die angereisten Datenschützer, die für ihre zweitägige Unterweisung 1824,– DM berappen mußten, fanden es pikant, daß Cheshire ihnen hymnensingend den Einbruch in eine amerikanische Datenbank vorführte – live per Hoteltelefon. Was sie nicht wußten: Richard Cheshire war noch tags zuvor Stargast eines bundesdeutschen Hacker-Happenings gewesen.

Akademische Republikmuffel als Sicherheitsrisiko

Die Unterscheidung zwischen gutmütigen Hackern und böswilligen Crackern mag für die USA eben noch angehen. In den bundesdeutschen Landen liegen die Dinge verzwickter. Die ganz jungen Computerfreaks sind derzeit noch voll damit ausgelastet, schwarz kopierte Videospielprogramme zu dealen – Treffpunkt: die Computer-Ecke im Kaufhaus, da läßt sich der Stoff gleich auf seine Qualität prüfen. Telefon-Hacking ist ihnen noch fremd, schließlich fehlt ihnen das öffentliche Datennetz, wie es die USA nun mal haben. Doch kommt Zeit, kommt Btx. Und damit ein frei zugängliches Computer-Netzwerk, eine grandiose Herausforderung für alle Home- und Personalcomputer.

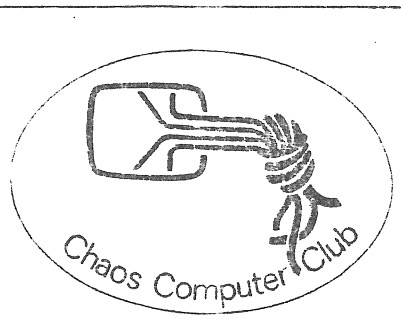
Weit aktuellere Sorgen machen den Sicherheitsexperten bei Post und Industrie die reiferen Jahrgänge: linke und bunte Republikmuffel, nicht selten mit akademischer Ausbildung. Das sind Leute, die ihr atomstromendes E-Werk mit groschenweise überwiesenen Stromrechnungen nerven. Oder Päckchen und Briefe grundsätzlich mit Zehnpfennigmarken bepflastern („es könnte ja eine ungestempelt bleiben!"). Zwischendurch demonstrieren sie gegen die Pershing und für den Frieden.

Die ganze Verkabelung und Verdatung hängt diesen Typen schon zum Halse raus, ehe sie recht begonnen hat: Die Menschen würden dadurch nicht nur ihre Arbeit, sondern auch ihre Freiheit und die Fähigkeit zum miteinander Reden verlieren, behaupten sie. Technischer Fortschritt ist ihnen schlechterdings ein Greuel, und sie lauern auf jede Gelegenheit, ihm ein Bein zu stellen. In den Zeitungen und Zeitschriften dieser Polit-Szene stehen Hinweise auf das Wandern in Datenbanken, Löschen und Verändern von Computerspeichern und das Knacken von Paßwörtern ebenso hoch im Kurs, wie Hinweise auf Schwächen des Telefonsystems der Bundespost. Auch das Spezialmagazin „TAP" hat ein Pendant im deutschen Informatik-Untergrund bekommen: Die „Datenschleuder", Organ des „Chaos Computer Clubs CCC", berichtet mit bemerkenswertem Sachverstand über Datex-Anschlüsse, Mailboxen oder billige (und natürlich verbotene) Telefon-Modems. Ganz lebensnah geben die Chaoten Hinweise, wo denn der Sand am besten ins Getriebe der Datenwelt zu schütten ist. Beispiel: „Durchwahlnummern zu Modem-Anschlüssen in Firmen lassen sich leichter finden, wenn man die Durchwahl zum Rechenzentrum kennt (erhält man beider Vermittlung). Dann die Ziffern auf- oder abrunden, und schon piept es".

Die Compumaniaks freuen sich schon auf die offizielle Einführung von Bildschirmtext. Vielleicht ist etwas dran an dem Gerücht von dem Duplizierungsprogramm, mit dem sich der Speicher eines am Btx-Netz angeschlossenen Großrechners in Minutenschnelle vollknallen läßt („Schafft Arbeitsplätze in der EDV-Abteilung").
Der Londoner Hacker-Club tobt mit dem Commodore VC 64 schließlich auch schon im PRESTEL herum, da wird man den bundesdeutschen Bildschirmtext wohl auch noch mürbe kriegen.
Die Bundespost lacht nur, wenn solche Zweifel an der Sicherheit von Btx geäußert werden. Doch wie geschützt ist Bildschirmtext wirklich?

Horror-Visionen durch vorsätzliche Schädigungen

Bildschirmtext öffnet in diesem Frühsommer bundesweit seine Pforten. Der Informationsdienst, der mit sich reden läßt, bringt Computerleistung in jedes Wohnzimmer: vermittelt von der Ulmer Leitzentrale werden sich zahlreiche Großrechner und Datenbanken aus Industrie und Verwaltung an das Netz anschalten. Jeder, der ein Telefon und ein Fernsehgerät besitzt, kann mitmachen. Tastatur und Decoder für's TV-Gerät liefert der Fachhandel, die Post stellt dem gemeldeten Teilnehmer ein Telefon-Modem, die Schnittstelle zwischen dem digitalen Btx-Decoder und dem analogen Fernsprechnetz. Ein nur dem Benutzer bekanntes Paßwort und eine verdeckte elektronische Kennung im Modem bilden den Schlüssel zum System.
Der Datenschutz gehört zu den heißen Themen der Btx-Diskussion. Schließlich wäre es hier so leicht wie nie zuvor, ein umfassendes Persönlichkeitsprofil des Nutzers anzufertigen. Welche Zeitungen liest er, was kauft er ein, wem teilt er was mit. Daß dies – außer Polizei und Verfassungsschutz – kein anderer tut, ist zur politischen Sorge geworden.
Doch neben diesem „Mißbrauch von innen" gibt es auch noch den „Mißbrauch von außen". Im einfachsten Fall ist das der unberechtigte Abruf gebührenpflichtiger Seiten auf Kosten eines anderen Teilnehmers. Lästiger wird's schon, wenn Anbieter mit eigener Rechneranbindung vorsätzlich geschädigt werden: betrogene Kreditinstitute, zerstörte Datenbanken und nicht mehr betriebsfähige Rechner etwa im Großversandhandel sind Horrorvisionen kommender Zeiten.
Wie sicher ist Bildschirmtext wirklich? Verfolgen wir doch einmal was bei der Eröffnungsprozedur, dem „log-on", geschieht. Drückt der Teilnehmer auf seiner Tastatur die „BT"-Taste, schaltet sich sein Fernsehgerät ein. Sein Telefon-Modem wählt jetzt selbsttätig die nächstgelegene Btx-Vermittlungsstelle an, die die Verbindung zum Teilnehmerrechner der Post herstellt. Von dort kommt dann – für den Nutzer nicht erkennbar – die Rückmeldung an das Modem. Gib mir mal Deine zwölfstellige Gerätekennung durch, damit ich überhaupt weiß, wer da anruft. Aus Grund dieser verdeckten Kennung sucht der Postrechner den Stammdatensatz des Teilnehmers heraus, der außer dieser verdeckten zwölfstelligen Hardwarekennung noch die offizielle Teilnehmernummer (künftig identisch mit der Telefonnummer) und das persönliche Paßwort enthält.
Nun will der Postrechner sicher gehen, daß sich da auch der Richtige bei ihm meldet. „Bitte Kennwort eingeben" liest der Btx-Nutzer auf seinem Schirm. Wählt er das nur ihm bekannte Codewort ein – es besteht aus vier bis acht Buchstaben oder Ziffern –, erscheinen natürlich nur Striche am Schirm, damit keiner mitlesen kann. Der Postrechner vergleicht das eingegebene mit seinem gespeicherten Kennwort. Stimmen sie überein, wird der log-on akzeptiert: der Teilnehmer wird freundlich begrüßt und erfährt Datum und Uhrzeit seiner letzten Dienstnutzung.
Er kann jetzt mit dem Seitenabruf beginnen. Erfolgt mehrere Minuten lang keine Eingabe, wird die Verbindung nach Vorankündigung automatisch getrennt.
Zweimal darf sich der Nutzer bei der Kennwort-Eingabe vertun, beim dritten Mal wird der Postrechner mißtrauisch und sperrt den Anschluß. Erst ein schriftlicher Antrag beim nächsten Fernmeldeamt bringt die Befreiung: im allnächtlichen Reorganisationslauf in der Ulmer Leitzentrale wird der Anschluß wieder entsperrt.
Vergißt ein Teilnehmer einmal sein Kennwort, dann geht die Datenwelt nicht unter. Er muß sich dann „irgendwie" gegenüber der Post identifizieren; über einen bundeseinheitlichen Telefax-Anschluß bekommt er dann von der Ulmer Zentrale ein neues vorläufiges Kennwort zugeteilt. Wieder Dienstzugriff, kann der Teilnehmer sofort dieses Kennwort durch ein neues, nur ihm bekanntes, ersetzen. Und wem ihm das alles so peinlich war, wird erstens jetzt sein Codewort auf einen Zettel schreiben und unter die Tastatur kleben.
Anbieter von Btx-Informationen können einzelne Seitenbereiche mit sensiblen Inhalten vor dem öffentlichen Zugriff schützen. Sie bilden „Geschlossene Benutzergruppen" (BGB oder „closed user groups"), deren Mitglieder ein zusätzliches, vom Anbieter zugeteiltes Codewort kennen müssen, wenn sie auf die geschützten Seiten zugreifen wollen. Der Postrechner weiß von diesem Sonder-



„In diesem Zeichen werden wir stören": Die Verdrahtung und Verkabelung ist einigen Republikmuffeln ein Dorn im linken Auge.

Die Hacker-Hymne

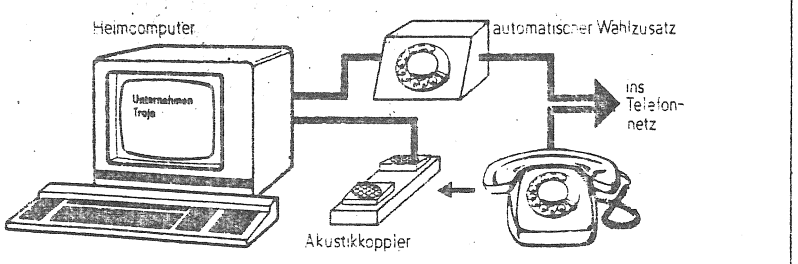
Zu singen nach der Melodie „Put another nickel in"

Gib ein neues Paßwort ein
Oft fliegst Du 'raus,
mal kommst Du rein
Schau genau beim Tippen zu
Wir hacken, hacken, hacken.

Find vom Chef die Freundin raus
Probiere ihren Namen aus
Tast Dich ran mit Ruh im Nu
Zum Hacken, Hacken, Hacken.

Begreife endlich das System
Dann hast Du es ganz bequem
Was Du willst, das tu', ja tu'
Du Hacker, Hacker, Hacker.

Amerikan. Originaltext von Cheshire Catalyst.
Ins Deutsche übertragen von einem Computer-Chaoten.



Werkzeuge für Datendiebe: Der automatische Wählzusatz hilft beim Aufspüren der Telefonnummer; Akustikkoppler und Telefon übernehmen die Datenübertragung.

tus des Teilnehmers und prüft beim Zugriff auf GBG-Seiten zweifach: Kennt der Teilnehmer das GBG-Codewort und darf er es laut Stammdatensatz überhaupt kennen?

Besonderen Wert auf Schutz vor unberechtigtem Zugriff legen natürlich die Geldinsitute, die sich am Service „Hombanking" beteiligen. PIN und TAN sollen dafür sorgen, daß keiner unberechtigt eines anderen Bankkonto mißbraucht. PIN ist die „Persönliche Identifikationsnummer", eine nur dem Kontoinhaber bekannte Geheimzahl, und TAN die „Transaktions-Nummer". Die TAN ist eine Zufallszahl, die für jeden Bankauftrag nur einmal verwendet werden kann. Sie wird dem Kontoinhaber von seiner Bank in Blöcken zu voraussichtlich 50 Stück zugeteilt und muß Nummer für Nummer verbraucht werden. Als weiteren Schutz vor Mißbrauch denkt man in Bankerkreisen über eine individuell zu vereinbarende Betragsobergrenze für Telebanking-Aufträge nach.

Rechenzentren, die vertrauliche Kundendaten via Btx zur Verarbeitung annehmen, werden gut daran tun, die „Gateways", die Übergangs-Seiten vom Postrechner zum eigenen System auf GBG-Status zu setzen. Wer dann noch sein persönliches Paßwort eingibt, kann sich nur in dem für ihn vorgesehenen Seitenbereich bewegen – das Leitseitenprinzip des Postrechners kann hier sinnvoll übernommen werden.

Eldorado für Hacker, Cracker und Caoten

Doch längst nicht alle externen Rechner werden diesen Sicherheitstandard bieten können. Großversandhäuser etwa müssen sich einen bedienerfreundlichen Btx-Zugang offenhalten, schließlich genügt bei einer normalen telefonischen Bestellung auch die Angabe der Kundennummer. Wer als externer Rechner-Anbieter nicht auf die 1985 lieferbare Kopplungssoftware von IBM warten möchte, wird sich den Verbindungstunnel zum Postsystem selbst zusammenzimmern müssen. Die Bundespost kümmert sich nicht darum, wie es hinter ihrer Gateway-Seite aussieht. Doch genau da liegt Anderland – das Eldorado für Hacker, Cracker und Chaoten. Zahlreiche Großrechner erinnern an ein altes Schloß mit vielen Zimmern und geheimen Gängen. Von der ursprünglichen Rechner-Architektur ist oft nicht mehr viel übrig: Zuviele Programmierer haben im Laufe der Jahre hier ein Programm ergänzt, da einen Fehler korrigiert und dort einen Trick ins Betriebssystem eingebaut. Da entstanden Schnittstellen zwischen völlig verschiedenen Programmpaketen. Sprünge und Verzweigungen, deren geheimen Sinn nicht einmal derjenige lüften könnte, der sie vor Jahr und Tag programmiert hat. Vielleicht liegt in irgendeinem Datenkeller sogar eine „logische Bombe", Ausgeburt eines betrügerischen Buchhaltergehirns, das die Entdeckung im Revisionslauf mehr fürchtet, als die Lahmlegung des ganzen Rechnersystems. Wenn die Bombe hochgeht, weil sie durch eine Prüfung angesprochen wurde, löst sie das große Datenchaos aus. Hoffentlich tritt kein Hacker versehentlich auf den Zünder.

Ganz oben im Speicher des alten Zahlenschlosses liegt vielleicht noch ein längst vergessenes Dienstprogramm. Irgendein Systemprogrammierer hat es da mal abgelegt, um bei Störungen nicht ständig die Mitarbeiter des Betriebes nach ihren Paßwörtern fragen zu müssen. Mit seinem Standard-Codewort („Test", „Syscall" oder gar „Joshua") übersteigt er alle Sicherheitshürden. Natürlich in jedem Rechner, der mit diesem Betriebssystem fährt.

Blühende Kinophantasie? Leider nein, die amerikanische Fachpresse weiß immer wieder von solchen Fällen zu berichten. In Deutschland nicht möglich? Auch falsch, schon im Feldversuch schaffte es ein Berliner Btx-Teilnehmer, das Alter seiner Großmutter im Computer eines Großversenders auf 200 zu trimmen.

Die Post dünkt sich trotz alledem knitz wie Rumpelstilzchen. Immerhin, so ein Sprecher der OPD Stuttgart, ist die Wahrscheinlichkeit, ein persönliches Kennwort herauszufinden, mit weniger als 1 : 100 000 000 noch geringer, als 6 Richtige im Lotto zu treffen".

Ganz so mühsam ist's in der Praxis dann wohl doch nicht. Sieht man einmal von den einfachen Fällen ab – der Mitarbeiter weiß es vom Chef, der Sohn guckt es dem Vater von den Fingern –, so hilft nicht selten etwas psychologisches Einfühlungsvermögen weiter. Vielen fällt als merkbares Paßwort nur der Name ihrer Freundin ein, ihr Geburtsdatum oder ein Computerbegriff. Auch Vornahmen aus „Dallas" und „Denverclan" rangieren in der Beliebtheitsliste ganz oben. In vielen Betrieben tuts auch einfach der Zunahme des jeweiligen Sachbearbeiters.

Hat ein unberechtigter Eindringling mit diesen Versuchen kein Glück gehabt, wird er wohl inzwischen Mitleid mit dem Anschluß-Inhaber bekommen haben. Der muß schließlich nach jedem dritten Fehlversuch die Entsperrung beantragen.

Dabei geht es mit ein wenig technischem Geschick viel einfacher: Man hört die Telefonleitung des Teilnehmers während des log-on ab. Nur physikalisch sehr Unbegabte klemmen sich hierzu galvanisch an den Telefonverteilkasten im Treppenhaus, eleganter ist die induktive Ankopplung an irgendeiner Stelle der Leitung. Die frequenzmodulierten Bitfolgen (FSK-Verfahren) enthalten neben dem Kennwort ja auch die verdeckte Hardware-Kennung des Modems. Füttert man einen tragbaren PC mit Akustik-Koppler mit diesen Daten, kann die Post an die Post von jedem beliebigen Telefon abgehen.

Fortgeschrittene Kriminelle können sogar trotz PIN und TAN die Telebank linken. Sie schalten sich in die Telefonleitung, tun mit ihrem Banditenrechner so, als ob sie der Postrechner seien, und fragen den Teilnehmer höflich nach den Geheimzahlen. Dann wechseln sie die Rolle, werden zum Teilnehmer und kontakten die Bank wegen der Überweisung selbst. Kontonummer des Empfängers und Betrag stehen zur freien Wahl.

Diese Idee war schon im Herbst 1983 in einer amerikanischen Armeezeitschrift zu lesen. Ihre Verwirklichung setzt allerdings gewisse Kenntnisse der Verkehrsvorschriften mit dem Postrechner voraus. Nachzulesen sind sie in den EHKP, den „Einheitlichen höheren Kommunikationsprotokollen" des Innenministeriums, die jede Buchhandlung für knapp 100,– DM besorgen kann (VIBIG-Verlag, Wiesbaden).

Nur Silberstreifen der Computersicherheit sichtbar

Wer uns nun vorhält, wir würden mit dieser Veröffentlichung zu computerkriminellen Handlungen ermuntern, hat noch nicht begriffen, daß die Mutwilligen in diesem Lande schon längst besser Bescheid wissen, als die Sicherheitsexperten und Datenschützer. Wenn hier der Teufel an die Wand gemalt wurde, dann mit der Absicht, der Vogel-Strauß-Mentalität bei der Computersicherheit einen Schock zu versetzen. Lösungsvorschläge, wie die verschlüsselte Datenübertragung oder die Chipkarte, sind allenfalls Silberstreifen am Horizont.

Hacker, Cracker und Chaoten werden all ihre Phantasie in ihre Home- und Personal-Computer packen. Der digitale Marsch auf die Datenfestungen der Republik hat schon begonnen.