Computer-Piraterie:

Marsch auf die Datenfestungen

Btx: Selbstbedienungsladen für Hacker?

Längst ist die Diskussion darüber entbrannt, ob Daten in Btx-Computern sicher vor unerlaubtem Zugriff sind. Galt die Sorge bislang einer unbändigen Neugier von Vater Staat und Btx-Anbietern, so kommt jetzt eine neue Sorge hinzu: die Hacker.

Für den eiligen Leser

Bildschirmtext ermöglicht es jedem, über das öffentliche Telefonnetz mit anderen Teilnehmern oder Datenbanken einen Informationsaustausch vorzunehmen. Kennungen und Codeworte sollen dabei garantieren, daß kein Unbefugter an die Informationen herankommt. Hacker – das sind Computerfreaks, die per Telefonleitung in fremde Computer eindringen – werden jedoch ihren Einfallsreichtum nutzen, um dennoch Btx-Computer zu knacken.
Droht uns das Daten-Chaos? Eine schlüssige Antwort kann auch der Beitrag nicht geben: Er beleuchtet vielmehr das Problem und zeigt Risiken des Btx so auf, daß es Btx-Teilnehmern mulmig werden kann.

Datenschutz bei Btx, das ist nicht nur für Informationsanbieter ein heißes Thema, sondern auch für jeden einzelnen privaten Teilnehmer. Sorglosigkeit ist hier fehl am Platz, denn wer hat es schon gerne, daß einem klammheimlich von einem unbefugten Btx-Teilnehmer das Konto erleichtert wird! Obwohl das bei uns noch eine Vision ist, sollte man sich darüber im klaren sein, daß „Hacker" zu einem Risikofaktor für die Teilnehmer am Btx-Dienst werden können.

Was heißt hier Cracker?

Eine Fachtagung der Leuro Seminar GmbH, München, machte es vor kurzem deutlich: Gastredner Cheshire Catalyst, ein gelernter Datenbank-Knacker aus USA, prophezeite den deutschen Btx-Teilnehmern düstere Zeiten. Und es ist zu befürchten, daß es stimmt, was Catalyst, der auch unter dem Pseudonym Richard Chesire bekannt ist, sagt, denn er ist ein ausgefuchster Profi.

Als die FUNKSCHAU in Heft 4/1984, Seite 73, über die Methoden von Datendieben berichtete, gab es für diese Personengruppe allein den Begriff „Hacker", der aus dem amerikanischen übernommen wurde und sich hier rasch eingebürgert hat. In Amerika ist man bereits feinsinniger geworden und unterscheidet zwischen Hackern und Crackern.

„Hacker", so definierte Cheshire Catalyst leutselig, „sind nur phantasievolle Kinder, die solange auf der Tastatur ihres Heimcomputers herumhacken, bis sie alle 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 Hackern fern.

Mit „Crackern", den wirklich rauhen 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, das sie mit einem erschlichenen Kennwort ihrem Nachbarn vom Bankkonto filzen, auch gleich aufs eigene Konto überweisen.

Richtig teuer wird es aber erst, wenn Cracker Industriespionage treiben – ohne daß es einer merkt: „Das sind die cleversten", meinte ein deutscher Rechtsexperte auf der Fachtagung.

Die Unterscheidung zwischen gutmütigen Hackern und böswilligen Crackern mag für die USA gelten, aber hierzulande liegen die Dinge anders. Die ganz jungen, zum Hacker-Nachwuchs zu zählenden Computerfreaks, sind derzeit noch voll damit ausgelastet, schwarz kopierte Videospielprogramme zu handeln. Treffpunkt ist die Computer-Ecke im Kaufhaus, da läßt sich der „Stoff" gleich auf seine Qualität prüfen.

Telefon-Hacking ist ihnen noch fremd, schließlich fehlt das öffentliche Datennetz, wie es die USA bereits haben. Doch kommt Zeit, kommt Btx – und damit ein frei zugängliches Computer-Netzwerk.

Hackerszene Deutschland: Warten auf Btx

Weit größere Sorgen machen den Sicherheitsexperten bei Post und Industrie die reiferen Jahrgänge, die nicht selten aus Staatsverdrossenheit heraus der Verkabelung und Verdatung den Kampf angesagt haben.

In den Zeitungen und Zeitschriften dieser Szene stehen Hinweise auf das Wandern in Datenbanken, Löschen und Verändern von Computerspeichern und das Knacken von Kennwörtern ebenso hoch im Kurs, wie Hinweise auf Schwächen des Telefonsystems der Bundespost.

Das Spezialmagazin „Datenschleuder", Organ des „Chaos Computer Clubs", berichtet z. B. mit bemerkenswertem Sachverstand über Datex-Anschlüsse, Mailboxen oder billige (und natürlich verbotene) Telefon-Modems. Ganz lebensnah werden da Tips gegeben, wo denn der Sand am besten ins Getriebe der Datenwelt zu schütten ist.

Vielen fällt als Kennwort nur der Name ihrer Freundin ein, ihr Geburtsdatum oder ein Computerbegriff. Auch Vornamen aus der Fernsehserie „Dallas" rangieren in der Beliebtheitsliste ganz oben. In vielen Betrieben tut's auch einfach der Zuname des jeweiligen Sachbearbeiters. Angst das Kennwort zu vergessen, prägt diese Einfallslosigkeit.

Technisch versierte Hacker haben noch andere Möglichkeiten, Kennworte herauszubekommen. Sie brechen das Telefongeheimnis und hören die Telefonleitung des Teilnehmers während der Eröffnungsprozedur ab. Die frequenzmodulierten Bitfolgen (FSK-Verfahren) enthalten neben dem Kennwort ja auch die verdeckte Hardware-Kennung des Modems. Füttert man einen tragbaren Computer mit diesen Daten, kann die Post an die Post von jedem beliebigen Telefon mit einem Akustik-Koppler abgehen.

Fortgeschrittene Hacker können theoretisch sogar in geschützte Datenbanken eindringen. Sie schalten sich in die Telefonleitung, tun mit ihrem Rechner 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 selber – wegen einer Überweisung versteht sich.

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.

Gefahr erkannt, Gefahr gebannt

Jeder Bericht über den Mißbrauch des Btx-Dienstes hat zwangsläufig etwas von einem zweischneidigem Schwert an sich. So könnte jetzt einer einwenden, daß durch Beiträge wie diesen Hacker erst auf ein neues Opfer aufmerksam werden. Dem läßt sich nur entgegenhalten, daß Hacker untereinander einen regen Informationsaustausch pflegen und auf derlei Veröffentlichungen keineswegs angewiesen sind. Stillhalten gemäß Vogel-Strauß-Manier wäre daher eine höchst wirkungslose Schutzmaßnahme.

Nein, wenn hier der Teufel an die Wand gemalt wurde, dann mit der Absicht, die Diskussion über den Datenschutz bei Btx auch auf das Risiko des Mißbrauchs von außen auszudehnen. Schließlich muß im Interesse jedes einzelnen sichergestellt sein, daß der Btx-Dienst nicht zum elektronischen Dietrich für Computer-Gauner, gleich welcher Art, zweckentfremdet wird. Da hört der Spaß auf.

Da das Unbehagen darüber, ob Bildschirmtext tatsächlich „sicher" ist, aber nun einmal geweckt ist, gilt es jetzt, Reaktionen der Post abzuwarten. Eine auf alle Fälle anzustrebende weitere Schutzmaßnahme wäre es, dem unerlaubten Zugriff auf fremde Daten endlich einmal das Image des Kavaliersdelikts zu nehmen.

Roland Dreyer

ZX-81-Softwaretip:

Da geht Editieren an die Nieren

Gerne werden beim ZX 81 Maschinenprogramme am Anfang eines Basic-Programms in einem REM-Kommentar untergebracht. Um Platz für das Maschinenprogramm zu reservieren, ist dann erst einmal die REM-Zeile mit irgendwelchen Zeichen zu füllen, und zwar so vielen, wie das Maschinenprogramm Bytes hat. Sicherheitshalber und weil das Abzählen lästig ist, gibt man aber oft ein paar Zeichen mehr als nötig ein.

Am besten probieren wir das einmal mit einem kleinen Maschinenprogramm aus, das eine Texteingabe wie mit einer Schreibmaschine zuläßt und „schneller" als eine Basic-Lösung arbeitet. Zuerst müssen wir das Eingabeprogramm (*Bild*) eintippen, es mit RUN starten und dann die folgenden Maschinencodes eingeben: 205, 187, 2, 125, 254, 255, 40, 248, 229, 193, 205, 189, 7, 126, 215, 205, 187, 2, 125, 254, 255, 32, 248, 201.

Nach dem Start mit GOTO 100 darf man jetzt losschreiben – selbst SPACE und NEWLINE funktionieren wie bei einer Schreibmaschine! Bei SHIFT-Eingaben ist jedoch Vorsicht geboten, denn mehrere von ihnen (z. B. EDIT, **, oder die Cursortasten) führen zum Absturz.

Oftmaliges Betätigen von NEWLINE führt zum Abbruch mit der Fehlermeldung 5 (Bildschirm voll). Zum Maschinenprogramm, das lediglich zur Demonstration dient, sei nur gesagt, daß es so kurz ist, weil die im ROM enthaltenen PRINT- und INKEY$-Routinen mitbenutzt werden.

Soweit wäre noch alles in Ordnung. Nur sind in Zeile 10 gewiß noch einige überflüssige A's stehengeblieben. Also rufen wir die Zeile mit EDIT auf, und löschen wir der Schönheit halber diese A's. Jetzt ist das Programm perfekt, nur – es läuft nicht mehr!

Tücke des Objekts ist der 14te Code unseres Maschinenprogramms: 126. Dieser Code meldet dem Betriebssystem, daß die folgenden fünf Codes (Bytes) als Basic-Gleitkommazahl anzusehen sind. Für das Betriebssystem haben diese Bytes in einer REM-Zeile aber nichts zu suchen. Der ZX 81 merkt das schon beim bloßen Aufrufen der Zeile 10 mittels EDIT und wirft alle sechs Bytes einfach aus dem Programmspeicher raus.

Mit einem dem eigentlichen Maschinenprogramm vorangestellten Code 126 (das entspricht dem Z-80-Befehl *ld a,(hl)*) läßt sich damit das Maschinenprogramm vor fremden Editierversuchen schützen. Ruiniert doch jeder Versuch das Programm, indem die ersten Bytes auf Nimmerwiedersehen verschwinden.

Damit man nicht in die eigene Falle tappt, empfiehlt es sich, POKE 16510,0 einzugeben. Dies setzt die Zeilennummer der ersten Programmzeile, hier steht normalerweise das Maschinenprogramm, auf 0. Das wiederum hat zur Folge, daß die Zeile zwar im Listing auftaucht und auch vom Computer akzeptiert wird, ein Editieren jedoch nicht mehr möglich ist (es sei denn, man gibt zuvor POKE 16510,1 ein).

Wolf-Dieter Roth

```
  10 REM AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAA
  20 FOR N=16514 TO 16537
  30 INPUT A
  40 POKE N,A
  50 NEXT N
  60 STOP
 100 RAND USR 16514
 110 GOTO 10
```

Eingabeprogramm: Dieses Programm bringt die im Text genannten Maschinencodes anstelle der A's in der REM-Zeile unter