DIE ZEIT – Nr. 49 – 30. November 1984

Ein Schlag gegen das System

Ein Computerclub deckt Sicherheitslücken im Btx-Programm der Post auf / Von Thomas von Randow

Wer sich in den kommenden zwei bis drei Jahren dem Btx-System anschließt, gehört wegen Dummheit bestraft." Dieses vernichtende Urteil über den neuen Service der Bundespost, Bildschirmtext, war vorige Woche auf der achten Datenschutzfachtagung in Köln zu hören – aus berufenem Munde. Gefällt hatte es der Vorsitzende der veranstaltenden Gesellschaft für den Datenschutz (GDD), Professor Reinhard Vossbein, nachdem ihm die Ausführungen eines Computerfreaks zu Ohren gekommen waren. Mit Witz und lockeren Sprüchen hatte Herwart („Wau") Holland vom Hamburger „Chaos Computer Club" (CCC) geschildert, wie es seinem 23jährigen Clubfreund Steffen Wernéry gelungen war, den Bildschirm-Dienst aufs Kreuz zu legen.

Eher tippe einer sechs Richtige im Lotto, als daß er sich illegal das Paßwort eines Btx-Teilnehmers verschaffen könne, hatten Bildschirmtext-Experten der Post geprahlt. Just das aber gelang den Hamburger Computerchaoten auf Anhieb. Ein Fehler, zünftig *bug* (engl. Käfer) genannt, im Computerprogramm des Systems machte es den Hackern kinderleicht. Daß etwas mit dem Programm nicht stimmte, war schon vielen Bildschirmtextanbietern aufgefallen.

Anbieter gestalten schirmfüllende Bilder mit Informationen darüber, was sie zu offerieren haben, Waren aus dem Versandkatalog, Urlaubsreisen, mit Kontoauszügen für Bankkunden oder schlichten Mitteilungen an Freunde. Diese „Seiten" können dann von – hierzu berechtigten – Btx-Teilnehmern abgerufen und die darin enthaltenen Fragen, etwa nach einer Flugbuchung, oder Geldüberweisung, auf der Tastatur am heimischen Btx-Zusatzgerät beantwortet werden.

Doch der Platz auf einem Fernsehbildschirm ist beschränkt; die Btx-Seite kann nur 1626 Zeichen fassen. Und damit der Gestalter beim Editieren weiß, wieviel Zeichen er jeweils noch in seinem Werk unterbringen kann, wird ihm diese Zahl am unteren Bildrand angegeben. Bis vor kurzem stimmte aber diese Angabe nicht – Programmierer sind notorisch schlechte Kopfrechner. Die Seite war schon voll, ehe die Zahl der verfügbaren Zeichen Null erreicht hatte. Aus diesem Grund erlebten viele Anbieter, was eigentlich nicht passieren darf, einen chaotischen Zeichenüberlauf.

Plötzlich geistern auf der Seite allerlei Wörter, Zahlen oder unverständliche Buchstabenfolgen. Der Grund für diesen Zeichensalat: Der Schöpfer des Btx-Programms hat offenbar vergessen, für die „Müllabfuhr" zu sorgen, nämlich dafür, daß überschüssiger Text vom Programm ignoriert oder irgendwie beiseite geschafft wird. Darum schieben die zuviel getippten Zeichen Teile aus dem Programmschreiber ins Bild; und die sind, wie die Hamburger Hacker herausfanden, manchmal verräterisch. Sie können ausgerechnet das Geheimnis preisgeben, daß ein Btx-Teilnehmer strengstens zu hüten hat, seine Kennung. Dieses Paßwort ist der Schlüssel für den Zugang zum System. Damit kann zwar noch niemand ein fremdes Bankkonto plündern, aber doch eine Menge Unfug stiften. Waren können bestellt, Urlaubsreisen gebucht, Zeitschriften abonniert werden. Für den dabei entstandenen Schaden haftet laut Vertrag der rechtmäßige Besitzer des Sicherheitscodes.

Steffen Wernéry und seine Genossen brachten – der Club ist eingetragener Anbieter – Btx-Seiten in Massen zum Überlauf und studierten dann die Geisterzeichen auf dem Bildschirm. Darunter entdeckten sie das Paßwort „usd 70000" der Hamburger Sparkasse (Haspa). Damit ließ sich veranstalten, was die Chaoten lange geplant hatten, eine eindrucksvolle Demonstration der Unzulänglichkeit des Bildschirmtextes. Sie richteten eine „Spendenseite" ein. Anbieter dürfen für den Abruf ihrer Seiten eine Art Schutzgebühr oder Spende verlangen, die jedoch nicht höher als 9,99 Mark sein darf. Wer eine solche Seite aufruft, dessen Konto wird automatisch mit der Gebühr belastet. Mit dem Sparkassen-Paßwort riefen die Hacker jetzt ihre eigene kostenpflichtige Seite ab – und 9,97 Mark waren verdient.

Dies sollte möglichst oft geschehen, weshalb ein Heimcomputer dafür programmiert wurde, die Seite laufend automatisch aufzurufen. Er tat es brav, und während sich die Clubmitglieder anderen Tätigkeiten widmeten, klingelte alle drei Sekunden die Kasse. Von Sonnabend 18 Uhr bis Sonntag 13 Uhr kamen insgesamt 135 000 Mark auf das Clubkonto. Die freilich überwiesen sie der Haspa zurück.

Einen *hack* haben amerikanische Studenten, lange schon bevor Computer populär wurden, die Art von Streich getauft, mit der Technik ausgetrickst wird. Legende ist der *hack* von Captain Crunch geworden, einem Studenten, der seinen Namen einer Cornflakes-Sorte entlehnt hatte. Den Packungen dieser Frühstückskrümel lag eine kleine Plastikpfeife bei, die zufällig exakt auf 2600 Hertz gestimmt war. Im amerikanischen Fernsprechsystem, das hatte Captain Crunch herausgetüftelt, ließ diese Frequenz, wenn sie ins Mikrophon des Telephonhörers gepfiffen wurde, den Gebührenzähler abfallen.

Der Trick mit den kostenlosen Ferngesprächen sprach sich schnell herum; er machte die Cornflakes-Firma reich und die Telephongesellschaft arm. Jedenfalls fand sie sich in argen Schwierigkeiten. Es galt den schwer ermittelbaren Verlust gegen eine teure technische Änderung im kontinentalen Netz abzuwägen. Bell entschied sich für die zweite Option.

Ein solcher Schlag gegen ein Computersystem vermittelt einen köstlichen Triumph, der den finanziellen Vorteil, der manchmal damit verbunden ist, weit überwiegt, ein Befreiungsschlag ist es, der uns für ein paar Augenblicke der Apparateherrschaft entwindet. In den dreißiger Jahren beleuchteten Hamburger Schrebergärtner kostenlos ihre

…ten den Code: Hacker Herwart Holland (links) und Steffen Wernéry Aufnahme: Sigmund v. Heydekamps

Häuschen. Stromlieferant war die nahestehende Antenne des starken Rundfunksenders, dessen Energie mittels eines simplen Sperrkreises in die Lampen umgeleitet wurde. Jahrelang blieb dieser *hack* unentdeckt – und als er schließlich ruchbar wurde, setzte er eine juristische Grundsatzdiskussion in Gang: Sind Radiostrahlen eine bewegliche Sache im Sinne des Gesetzes?

Anonym blieb der Tüftler, dem vor knapp zehn Jahren der *hack* mit den ersten Tastatur-Münzfernsprechern der Firma SEL eingefallen war. Gebraucht wurde dafür ein Feuerzeug mit piezoelektrischer Zündung. Wer kostenlos telephonieren wollte, begab sich in eine Fernsprechzelle mit dem SEL-Münzer, warf ein Fünfmarkstück ein und rief seinen Partner an. Ehe jedoch das ganze Geld verbraucht war, mußte das Feuerzeug in der Nähe der Tastatur geknipst werden. Dessen Funke verstörte die Elektronik erheblich, die daraufhin mutmaßen mußte, das Gespräch sei gar nicht zustande gekommen, und deshalb – *in dubio pro compartícipte* – den Fünfer wieder herausgab. In sämtlichen Münzfernsprechern jener Type mußten die Logik-Platinen ausgetauscht werden.

Für das Opfer ist der *hack* nicht nur lästig, sondern in der Regel ein Lehrstück, das technische Designfehler offenbart. Freilich nimmt mit dem Komplexitätsgrad des Systems auch der mögliche Schaden zu, der schon beim ersten *hack* angerichtet werden kann. So ist es eher ein Wunder, daß bisher die Spielchen der Btx-Hacker harmlos abgelaufen sind. Immerhin legten sie die Kläglichkeit des Bildschirmtext-Designs in einer Deutlichkeit bloß, die nichts zu wünschen übrig läßt.

Im Ursprungsland des Btx, Großbritannien, machten sich Hacker einen Spaß daraus, Prinz Philipps elektronischen Briefkasten zu knacken. Diese Btx-Briefkästen, *Mailbox* genannt, sind ohnehin merkwürdig konstruiert. Bildschirmtext-Post, die schon darin abgeworfen ist, kann dennoch nachträglich vom Absender umgeschrieben werden. Jede Mailbox kann sogar völlig unbrauchbar gemacht werden. Dazu muß nur – auch das haben die Hamburger Chaoshacker ausbaldowert – am Ende einer Seitenedition der Befehl stehen, den ganzen Aufruf zu wiederholen. Die so präparierte Seite taucht dann immer wieder auf. Das tut sie auch in dem Briefkasten, an den sie geschickt wird, mit dem Erfolg, daß nichts anderes mehr herausgeholt werden kann. Nur die Post vermag diesen Teufelskreis zu sprengen.

An das Bildschirmtextsystem läßt sich auch ein Mikrocomputer anschließen. Doch wehe dem, der damit ein auf seinen Gerätetyp spezialisiertes Crashprogramm aufruft. Es läßt den Computer abstürzen und vernichtet die in ihm gespeicherten Programme. Da hilft nur: Computer aus- und wieder einschalten. Das vernichtende Programm bietet sich als harmlose Bildschirmseite an. Raffinierte Hacker haben sie gar als Zeitbombe gestaltet. Erst nach einer Weile, wenn die zumeist mit albernen Sprüchen beschriftete Seite längst vergessen ist, bricht das Gerät zusammen, so daß die Ursache womöglich nicht mehr ermittelt werden kann.

All dies hätte der Bundespost schon lange eine Lehre sein müssen, ehe ihrem Lieblingskind Bildschirmtext Anfang letzter Woche die schallende Ohrfeige mit dem Sparkassen-Trick erteilt wurde. Das bißchen Flickwerk, das sie bislang nach jedem bekanntgewordenen Btx-*hack* veranstaltet hat, war offensichtlich unzureichend. Ein Programm, daß soviel Bereinigung braucht, ist hoffnungslos verpestet.

Fraglich ist, ob sich die Post beim Einrichter des Systems, IBM, schadlos halten kann. Um die Lieferung eines neuen Computerprogramms wird der „blaue Riese" kaum herumkommen. Und bis das fertig ist, dürften die zwei bis drei Jahre vergehen, die wohl Datenschützer Reinhard Vossbein meinte, als er jeden für sträflich dumm erklärte, der vor Ablauf dieser Zeit am Bildschirmtext teilnimmt.

Das wissen die Postler natürlich, und es schmerzt sie besonders deshalb, weil Btx gerade die letzten politischen Hürden auf dem Weg zur allgemeinen Einführung überwunden hatte. Weh tut es auch, da ohnehin das Interesse am neuen Kommunikationsmedium dürftig ist. Den optimistischen Voraussagen des Ministeriums entsprechend müßte Btx jetzt um die 150 000 Teilnehmer haben. In Wahrheit sind es knapp 19 000, davon 3000 Anbieter.