

Btx-System lieferte Hackern das Paßwort nicht

CW-Bericht, Claudia Marwede-Dengig

BONN/BERLIN — Vorläufig letzter Akt im Verwirrspiel um das Hamburger Hackerspektakel: Die Post hat festgestellt, daß der Chaos Computer Club (CCC) nicht durch den — vorhandenen — Programmfehler an Kennung und Paßwort des Btx-Anschlusses der Hamburger Sparkasse (Haspa) gelangt ist. Vielmehr sei zu vermuten, daß der CCC beides auf einer öffentlichen Btx-Vorführung der Haspa „ausgespäht“ hat. Immerhin ist es aber den Chaoten gelungen, auf diese Weise sich selbst und das neue Medium in die Schlagzeilen zu bringen.

Die Bundespost selber hat freilich — und nicht zum ersten Mal — durch ihre Informationspolitik mit dazu beigetragen, daß Bildschirmtext neuerlich ins Gerede gekommen ist. Einen Tag nach der Hacker-Demonstration in der ZDF-Sendung „Heute Journal“ mußte sie einen Softwarefehler (IBM-Sprachregelung: „eine isolierte Programmsituation“) einräumen.

Gleichzeitig verwies das Ministerium aber auch darauf, daß es sich bei dem Btx-Anschluß der Haspa um einen Vorführanschluß handele, der „freizügig“ geschaltet und somit nicht über Anschlußkennung und Paßwort geschützt war, sondern nur durch das persönliche Kennwort. Im Zusammenhang mit dem „Seitenüberlauf“ — so Eric Danke, Btx-Ver-

antwortlicher im Postministerium — habe nach dem damaligen Wissensstand „die theoretische Möglichkeit“ bestanden, daß die Hacker tatsächlich auf diese Weise in den Besitz des Paßwortes gelangt seien.

Die Chronik der Ereignisse, wie sie sich dem unbefangenen Beobachter jetzt darstellt:

Am 12. November meldet ein Berliner Btx-Anbieter der Post, daß beim Abruf einer bis ins letzte Bit vollgepackten Seite plötzlich die Adresse eines ihm völlig fremden Btx-Teilnehmers erschienen sei. Daraufhin versucht das Fernmeldetechnische Zentralamt (FTZ) in Darmstadt nach Auskunft von Danke den Fehler zu

Fortsetzung auf Seite 2

CW-Umfr.
Keßheit

„Ein Gesellschaft besaunders automatische Zeitpunliert.“ Im Umfrage zu Dr. Eberha führer de GmbH, di Rauch weit als Symbol gegen eine Welt sehen ten sich 33 an der grö me, die von CHE bish („Man stell men blühte

COMPUTERWOCHE *aktuell* COMPUTERWOCHE 14. Dezember 1984

Fortsetzung von Seite 1

Btx-System lieferte Hackern das Paßwort nicht

reproduzieren. Ergebnis: Man stößt auf Teile von Teilnehmerseiten, nicht jedoch auf persönliche Kennwörter von Teilnehmern. Die Post vermutet zunächst einen Datenbankfehler, was sich jedoch als nicht richtig erweist.

Der Berliner Anbieter, der den Fehler entdeckt hatte, kennt einige Mitglieder des Chaos Computer Clubs. Telefonisch berichtet er den Hamburgern von den Programmfehlern.

Am 15. November hält CCC-Mitglied „Wau“ Holland auf der „Dafta“ in Köln einen Vortrag über die Schwächen des Btx-Systems und darüber, wie dieses zu überlisten sei. Nach der detaillierten Schilderung des Softwarefehlers war man sich, wie Danke im nachhinein bekennt, spätestens jetzt bei der Post darüber im klaren, „daß etwas passieren mußte“.

Am 16. November, einem Freitag, und am darauffolgenden Wochenende wurde im FTZ alles darangesetzt, den Fehler aufzufindig zu machen.

Am Montag, den 19. 11., sperrt die Post die mit dem Fehler zusammenhängenden Systemfunktionen. Systemlieferant IBM wird aufgefordert, umgehend für Abhilfe zu sorgen. Dies geschieht Danke zufolge noch am gleichen Tag. Am nächsten Tag prüft die Post die neue Softwareversion und verteilt diese dann noch am Mittag im Btx-Netz.

Ebenfalls am Montag — und zwar um 8.30 Uhr morgens — haben sich „Wau“ Holland und seine Mannen beim Stellvertreter des Hamburgischen Datenschutzbeauftragten angesagt, um die am Wochenende gewonnenen „Erkenntnisse“ über die Schwachstellen im Btx-System zu demonstrieren. Die Sache hat allerdings einen Haken: Der Computer Club kann den Fehler nicht reproduzieren.

Post prüfte erst nach Fehlerrückmeldung genauer

Am Montagabend flummert dann im ZDF-Heute-Journal die Hackerinszenierung, dieses Mal allerdings in der Wohnung eines CCC-Mitglieds aufgenommen, über die Mattscheibe.

Am Dienstag, den 20. November, sieht sich die Post auf Grund der Ergebnisse des vorangegangenen Tages „unter Zugzwang gesetzt“ (O-Ton Eric Danke) und bezieht sich, die bereits erwähnte Stellungnahme zu formulieren.

Erst danach und nachdem die neue Software ins Netz geschleust worden ist, prüft die Bundespost die Vorkommnisse genauer — und stellte anhand ihrer für die gebührenpflichtigen

Seiten gesammelten Abrechnungsdaten fest, daß die Hacker nicht nur mit dem persönlichen Kennwort der Haspa gearbeitet hatten, sondern auch mit deren Kennung. Da aber nach Auskunft des Ministeriums die beiden Sicherungsmechanismen in getrennten Dateien gehalten werden, hätten trotz des festgestellten Softwarefehlers unmöglich Paßwort und Kennung auf ein und derselben Seite auftauchen können, wie die Chaoten immer behauptet hatten. Sie mußten also auf andere Art und Weise an die beiden Dinge gekommen sein. Dazu Heinz

dem System „über die Schulter sehen“ und gibt damit unbeabsichtigt aufmerksamen Beobachtern Gelegenheit, sich Kennung und Paßwort zu merken. Dieser fahrlässige Umgang mit den Sicherungsmechanismen ist vor allem bei den sogenannten Vorführanschlüssen häufig anzutreffen.


Chipkarten-Befürworter hätten Nutzen

Im vorliegenden Fall bleibt aber noch die Frage des „Cui bono?“. Abgesehen von der bundesweiten Publizität, die sich die CCC-Mitglieder durch ihren Coup verschafft haben, könnten Nutznießer diejenigen sein, die das derzeitige Btx-System als unsicher darstellen wollen und als Abhilfe die beschleunigte Einführung der Chipkarte propagieren.

In diesem Zusammenhang erscheint es mehr als bemerkenswert, daß Hacker „Wau“ Holland für die Kennung „Dafta“ von einem Mitglied der veranstaltenden Gesellschaft für Datenschutz und Datensicherung (GDD) angeheuert wurde, das zugleich auch bei der Scientific Control Systems GmbH in deren Bonner Dependence in Lohn und Brot steht. SCS berät die Bundespost bei der Einführung der Chipkarte.

Anzeige

Steigern Sie Ihre Maxell Datenlager die Zuverlässigkeit



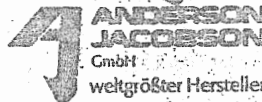
Erwin Riemann, Geschäftsführer der Bildschirmtext-Anbieter-Vereinigung e. V., Berlin: „Der CCC hat den Softwarefehler, der zweifellos vorhanden war, als Aufhänger genommen, um zu demonstrieren, daß das System noch nicht fehlerfrei läuft und was man damit machen kann. Im Grunde genommen waren es jedoch zwei völlig getrennte Dinge, die da vermengt wurden.“

Tatsächlich ist es nach Auskunft von Btx-Experten in einem bestimmten Fall — und ohne eine „freizügige“ Schaltung — nicht sonderlich schwer, gegenüber dem Btx-Rechner der Post in die Identität eines anderen Teilnehmers zu schlüpfen und zu dessen Lasten etwa gebührenpflichtige Seiten abzurufen.

Voraussetzung dafür ist zum einen ein Anschluß, der nicht über eine Btx-Anschlußbox mit automatischer Hardware-Kennung verfügt, sondern der mit dem Modem D 1200 S und einer Software-Kennung arbeitet. Hierbei müssen Kennung und Paßwort per Hand eingegeben werden.

Voraussetzung Nummer zwei: Der betreffende Btx-Teilnehmer läßt sich bei seiner Identifizierung gegenüber

AKUSTIK-KOPPLER
FTZ und VDE geprüft
Integriertes Mikrofon



Im Luchsfeld 5 - 5060 Bergisch Gladbach 1
Telefon (0 22 04) 5 30 51-53 - Telex 8 87 798

IBM-PC-Erfolg '84

Aus einem Werbebrief der Computer-Partner PC Vertriebsgesellschaft mbH, Hamburg, unter dem Motto „Große Computer Weihnachtsaktion 1984“: „Computer-Partner bietet für Sie und die Mitarbeiter Ihres Hauses, auf vielfachen Wunsch, stark reduziert den „IBM PC“ und den „Portable PC“ zum Sonderpreis an. Solange der Vorrat reicht! Bestellen Sie sofort!“