Morgenpost 22. 11. 1984

177

Seite 3

Wie der Chaos Computer Club Post und Sparkasse überlistete

Von Christian Personn

Hamburg – Der elektronische Bankraub, bei dem ein Hamburger Computerclub die Hamburger Sparkasse per Billig-Computer für eine Nacht um 135 000 Mark erleichterte, zeigt: „Btx" (Bildschirmtext) ist für Mißbrauch offen wie ein Scheunentor.

„Von den 135 000 Mark, die wir der Haspa abgezapft haben, wurde kein einziger Pfennig behalten", sagt Wau Holland (32) vom Hamburger „Chaos Computer Club" (CCC).

Mit dem üblichen Trick hatten die Computerknacker das Btx-System überrumpelt: Sie fütterten den zentralen Großrechner der Post so lange mit Informationen, bis dieser total überlastet nur noch „Daten-Müll" ausspuckte. Alle möglichen Informationen wirbelten zusammenhanglos über den Mini-Bildschirm der „Computer-Chaoten": Für eine zwölfstellige Kennummer mit drei Nullen am Anfang interessierten sich die Tüftler am meisten. „Zahlenstruktur und Handkennung zeigten uns schnell: Hier handelt es sich um Deutschlands größte Sparkasse", erzählt der Sprecher des Computerclubs.

Mit dem „Zufallsfund" wurde aus den Computeramateuren in wenigen Sekunden selbst die Hamburger Sparkasse: Durch die eingefangene geheime Anschlußnummer und das Paßwort konnte sich der Club gegenüber der Post nun als „Haspa" ausgeben. Dann ging alles problemlos: Als „Haspa" rief ein Computer-Freak eine gebührenpflichtige Btx-Seite des Chaos-Computer-Clubs an – immer wieder. Und über dieses automatische Wiederholungsprogramm wurden jedes Mal 9,97 Mark dem CCC gutgeschrieben. Über Nacht kamen so insgesamt 135 000 Mark zusammen.

„Wenn wir gewollt hätten, wären es gut und gerne eine Million geworden. Aber wir brauchten unsere Geräte auch noch für was anderes", sagt Holland. Grundsätzlich ging es dem Computerclub bei der Aktion aber um das Aufzeigen der Risiken beim Btx-System. Hauptkritik der Computerknacker: Der unkontrollierte Zugang für Unbefugte.

„Seit einem halben Jahr weisen wir auf

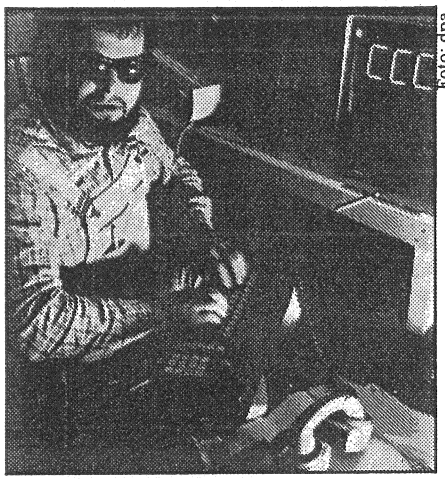

Foto: dpa

Chaos-Computer-Hacker Manfred „Wau" Holland an seinem „Arbeitsplatz"

die Mißbrauchsmöglichkeiten bei Btx hin, mit denen Millionen Mark von Banken abgezapft werden können. Nun mußte der Post eben einmal der Beweis erbracht werden", begründet Holland den Computer-Klau.

Mit der Aktion des „CCC" ist das erste Mal ein schwerwiegender Fehler in dem erst seit einigen Monaten bundesweit arbeitenden Bildschirmtext-Dienst der Post aufgedeckt worden.

Rund 20 000 Teilnehmer nutzen derzeit den Bildschirmtext-Service: Wer das notwendige Zusatzgerät an seinem Fernseher hat, kann vom Wohnzimmer aus beispielsweise Autos bei Versandhäusern ordern oder seine Kontoauszüge abrufen. Die Post registriert und rechnet ab. Die Banken sind dabei einer der Hauptanbieter im System.

Ein elektronischer Bankbetrug wie jetzt bei der Haspa ist nach Angaben des Bundesverbands Deutscher Banken in Köln bis jetzt noch nie vorgekommen: Die Bundespost will jetzt die Sicherheit bei Btx gegen Computerpiraten „noch weiter erhöhen".

Schon seit Jahren tummeln sich diese, meist jüngeren „Hacker" in den Datennetzen. Nacht für Nacht führen rund 3000 aktive Hacker mit technischer Respektlosigkeit ihren Kampf gegen die Rechner im deutschsprachigen Raum. In den USA, dem Mutterland der Hacker, zapfen sie regelmäßig Datenbanken an oder vernichten aus purer Lust am Spaß riesige Informationspools.

Der „CCC" dagegen versteht sich eher als eine Art „Robin Data": „Wenn die Post nicht über die Gefahren von Btx aufklärt, müssen wir es eben tun", sagt Holland. Die Hamburger Sparkasse überlegt nun, ob sie die Bundespost wegen mangelnder Sicherheitsvorkehrungen verklagen soll. Für die 300 Hacker, die sich zum Jahresende in Hamburg zwecks Informationsaustausch über den „Daten-Untergrund" treffen, gibt es also genug Gesprächsstoff.

Wie man ins Btx-System „einsteigt"

Im Normalfall ist der Btx-Benutzer über ein Modem (das Computersignale in übertragbare Töne umwandelt) von der Post per Telefon an die Btx-Zentralcomputer angeschlossen. Wählt der Btx-Teilnehmer die Zentrale an, gibt dieses Modem automatisch eine Teilnehmer-Kennung an den Rechner. Im zweiten Schritt muß sich der Benutzer dann noch über ein Kennwort identifizieren.

Ein „Hacker", der in das Btx-System einsteigen will, braucht nur ein (verbotenes) Modem, das keine automatische Kennung aussendet. Bauanleitungen für solche Modems gibt es bereits ab zehn Mark.

Über dieses Modem meldet sich der Hacker dann mit einer beliebigen Kennung – beispielsweise der der Haspa. Verfügt der illegale Besucher dann noch über das passende Schlüsselwort, dann glaubt der Post-Computer: Anwender Haspa ist am Draht.

Wau Holland: „Die erste Zahl – das ist praktisch der Kellerschlüssel – das Kennwort ist dann der Fahrradschlüssel." Der „Hacker" muß nur noch aufschließen und wegfahren.