Erweiterte Kommunikation in Bildschirmtext

Vandale im „Volksdatennetz“

Berlin (taz).
Anti-Verkabelungsgruppen sind von der Theorie zur Praxis übergegangen. Nach dem Vorbild der US-amerikanischen Hackers beginnen sie, die bundesdeutschen Datensümpfe auszuloten. Hervorragend geeignet dafür ist die von Post und Wirtschaft vorangetriebene Totalvernetzung für Bildschirmtext.

Im Telefonnetz der Bundespost tun sich Hacker ziemlich schwer, weil die aufwendige Amtsbautechnik unzulässige Eingriffe von außen fast unmöglich macht.

Fast schon kinderleicht dagegen ist das vagabundieren im neuen „Volksdatennetz“ Bildschirmtext (Btx). Abgesehen davon, daß schon der Datenschutz der personenbezogenen Daten in Artikel 9 des **Staatsvertrages über Bildschirmtext höchst unzureichend geregelt ist, fehlt es an der** notwendigen Datensicherheit im System selbst.

In der Diebold-Risiko-Analyse von Btx zeigen sich dann auch die vier Schwachstellen des Systems:

1. mögliches Abhören von Kommunikationsleitungen,
2. unerlaubte Nutzung des Systems,
3. unerlaubter Zugriff zu Daten und Programmen und
4. Störung von Transaktionen und Verfälschung von Nachrichten durch Einspielen falscher Daten.

Der größte Schwerpunkt liegt in der Telefonleitung. Die Post ist bei der Planung des „Volksdatennetzes“ blauäugig davon ausgegangen, daß nur von ihr genehmigtes Zubehör, wie Modems und Decoder, eingesetzt werden (Für Anfänger: Modems sind die Btx-Empfänger, die am Telefonanschluß hängen und in die die Verbindung zum Fernsehen eingestöpselt wird; der Decoder verwandelt das elektronische Signal in ein Fernsehbild und ist normalerweise im Fernseher eingebaut - wenn er nicht durch z.B. einen Heimcomputer ersetzt wird, s.u. - d. Red.) Genau an diesem Punkt haben Hacker nachgehakt und Zubehör eingesetzt, das nicht den Postnormen entspricht. Mit überraschendem Erfolg.

Schon mit einem simplen Cassettenrecorder der über ein kleines Gummimikrofon mit dem Gehäuse des anrufenden Telefons verbunden ist, lassen sich Verbindungen mit dem Btx-Rechner der Post abhören, aufzeichnen und später auf dem eigenen Fernseher sichtbar machen. Wenn es sich bei der durchgeführten Transaktion beispielsweise um eine Überweisung auf ein anderes Konto gehandelt hat, kennt der Abhörende folgende Daten: Name des Kontoinhabers, Kontonummer, Geheimzahl, Transaktionsnummer, Paßwörter, Kontostand, Betrag der Überweisung und den Empfänger. Mit diesen Informationen kann er sich mittels einer neu aufzubauenden Verbindung mit dem Computer den Kontostand sowie die Transaktion auf dem Konto ansehen. Eine Überweisung kann er nicht vornehmen, da die abgehörte Transaktionsnummer nur einmal benutzt werden kann.

Falls aufwendigere Technik, wie beispielsweise der erweiterte MUPID-Rechner mit spezieller Software, eingesetzt wird, ist es ohne weiteres möglich, die Überweisung abzufangen, die Empfängerdaten und den Betrag zu ändern und mit der noch gültigen Transaktionsnummer an die Bank weiterzuleiten.

Um an diese Daten zu kommen, ist nicht unbedingt eine Verbindung mit der Leitung des Btx-Teilnehmers nötig. Fernsehsichtschirme erzeugen beim Bildaufbau eine elektromagnetische Strahlung, die bis einige Meter weit vor die Haustür reicht. Sie kann mit einer elektromagnetischen Spule abgehört und auf einem anderen Schirm dargestellt werden, allerdings nur, wenn in dem Raum nur ein Bildschirm in Betrieb ist. In sicherheitsempfindlichen Bereichen müssen deshalb immer mehrere Monitore sein.

Die Datensicherheit bei Btx basiert im wesentlichen auf der Verwendung von Paßwörtern, persönlichen Identifikations- oder Geheimnummern (PIN) und Transaktionsnummern (TAN).

Für die PIN wird verlangt, daß es sich nicht um das Geburtsdatum, die Kontonummer, auf- oder absteigende Zahlenreihen, Zahlenspiegel oder sechs gleiche Ziffern handeln darf. Wird fünfmal die falsche PIN eingegeben, erfolgt automatische Sperre des Kontos für Btx-Zugriff. Die zehnstellige TAN wird durch einen Zufallsgenerator ausgewählt und 100-stückweise dem Teilnehmer per Einschreiben zugeschickt. Wenn der Bestand auf 42 Stück gesunken ist, schickt der Computer neue, denn jede TAN kann nur einmal verwandt werden.

Die TAN wird den Banken noch einiges Kopfzerbrechen bereiten, denn für die von der Post angepeilte Zahl von fünf Millionen Teilnehmern am Btx wird ein Speichervolumen von fünf GByte bei den Banken allein für die TANs benötigt. Sehr schwer vorzustellen, ganz abzusehen von dem organisatorischen Aufwand.

Überhaupt haben die Banken reichlich Probleme mit Btx. Allein die Computer-Mißbrauch-Versicherungen verlangen unbezahlbare Prämien und decken nur Schäden durch eigene Mitarbeiter. Der ernsthafte Hacker hat es da wesentlich einfacher, sich vom Postrechner mit anderen externen Rechnern verbinden zu lassen. Die Zugangskontrollen sind spielerisch zu überwinden.

Es ist nicht unbedingt erforderlich mit Postmaterial nach Postnorm zu arbeiten. Das Postmodem - neuerdings Btx-Anschlußbox genannt - kann durch ein HAYES Modem und der zur Zeit schwierig zu beschaffende hochintegrierte Decoder durch den CEPT MUPID oder einen **Heimcomputer, z.B. Commodore oder IBM-PC ersetzt werden. Der Hacker, der** diese Materialien nutzt, wird wohl vergessen, seine Teilnahme am Btx bei der Post anzumelden. Falls er einen „alten“ Decoder nach der Prestel-Norm besitzen sollte, kann der sehr effizient für mögliche Verbindungen zu den Postrechnern in Österreich (0043/22908), Schweiz (0041/31320771), Niederlande (0031/70151515) und Finnland (0036/806097) benutzt werden. Bis mindestens Mai 1984 funktioniert es auch bei uns noch unter 030/1551, 040/441271, 0211/1075, 0611/550591, 0711/299181 und 089/228282. Danach werden die Telefonnummern bundeseinheitlich unter 190 bis 199 zu finden sein.

Mit einem lizensierten Btx-Anschluß und Post-Modem muß man nicht selbst wählen und benötigt die angegebenen Telefonnummern nicht. Das macht das Modem automatisch. Ebenso gibt es dem Btx-Rechner die eigene Telefonnummer auf Anfrage bekannt. Das HAYES bietet diese „Vorteile“ nicht. Da muß der Betreiber schon selbst dafür sorgen, daß die richtige Nummer angewählt wird und die Kennung des eigenen Apparates stimmt. Dafür läßt sich die dazugehörige Software gut für die Kommunikation auch mit anderen Computern einsetzen.

Zur perfekten Ausrüstung fehlen dann nur noch eine Emulatorenplatine, die die Ausgangssignale des Heimcomputers für Großrechner verständlich macht, und die Telefonnummern anderer Großrechner.

Pius