Gefahren für Btx durch „Hacker"

Auf die Gefahren für Btx durch „Hacker" wies bei der 8. Datenschutzfachtagung (DAFTA) in Köln Dipl.-Ing. Ulrich Kranz von der SCS in Essen hin.

Btx-Adressen und Passwörter werden laut Kranz schon auf der Hakkerszene getauscht. Der fahrlässige Umgang mit Passwörtern von freizügig geschalteten Btx-Teilnehmeranschlüssen sei deshalb besonders gefährlich.

Ein Trick, Spenden zu sammeln: Der Computer Chaos Club fordert seine Leser auf, bei Messen und Ausstellungen, bei denen Btx-Geräte in Betrieb sind, mal eben eine Spendenseite für DM 9,99 abzuschicken.

Bis zur Einführung der Chipkarte zur Zugangssicherung und Identifizierung vor allem für Homebanking sei die Absicherung durch PIN und TAN eine pragmatische Übergangslösung, meint Kranz. Nach seiner Ansicht stellt im übrigen das Sperren einer PIN nach mehrmaligem nicht autorisierten Zugangsversuch eine „schwere Belästigung des Nutzers dar."

Weitere Möglichkeiten für Hacker: Die grundsätzliche Möglichkeit, die Funktionen von Btx-Dekodern in Form von Software auf PCs abzubilden, könnte dazu benutzt werden, beim Anzapfen eines Btx-Dialoges dem Benutzer die Btx-Zentrale und der Zentrale den Benutzer vorzutäuschen.

Es wird häufig die Meinung vertreten, dies läge durch den hohen technischen Aufwand außerhalb der Möglichkeiten von Hackern.

Der finanzielle oder kriminelle Anreiz, den diese Manipulationsmöglichkeiten bieten, verbunden mit wachsendem Btx-Software-Wissen und rasch sinkenden Preisen für PCs und Modem lassen eine Betätigung von „Hackern" auch auf diesem Feld vermuten.

Manipulation am Modem

Deutlich war's im „Heute-Journal" zu sehen: bei der 8. Datenschutzfachtagung (DAFTA) in Köln (15./16. 11.) öffnete einer, der sich als „Hacker" bezeichnet, ein Btx-Modem, ohne das Siegel zu verletzen. Der „freie Berater" Wau Holland nahm sich zwar kein Post-Modem vor, um „keine auf die Finger zu bekommen", versicherte aber, die Methode sei identisch. Auf der Rückseite des Modems hebelte er mit Hilfe eines dünnen Metallstreifens und eines Schraubenziehers die Schließ-Noppen aus. Man könne dann, so Holland, aus dem offenen Modem das Kennungsteil ausbauen, es verändern oder ein neues einbauen. Auch sei das Verstellen von Funktionen dann problemlos möglich (etwa Freizügigkeit). Nach dem Schließen ist äußerlich keine Veränderung erkennbar.

Hamburgs Hackerstory

Über mangelnde Publizität konnten sich die Hacker vom „Chaos Computer Club" (CCC) in den letzten Wochen nicht beklagen. Ihr Coup, die Hamburger Sparkasse (Haspa) um 135 000 Mark zu erleichtern, ließ sie in die Schlagzeilen und Btx in Mißkredit geraten.

Die Hacker erklärten, sie hätten sich einen Softwarefehler im System zunutze gemacht. Dieser Fehler trete dann auf, wenn eine Btx-Seite beim Editieren bis zum Rand vollgeschrieben sei. Werde sie wieder abgerufen, tauchten Daten oder Seiten auf dem Schirm auf, die in keiner Beziehung zur Eingabe ständen.

So wollen die Leute vom CCC auch an die Teilnehmernummer und das Paßwort der Haspa gekommen sein. Mit Hilfe der Zugangskennung gaben sie sich dem Postcomputer gegenüber als Haspa aus und riefen am Wochenende mit Hilfe eines Kleinrechners immer wieder eine gebührenpflichtige Seite aus ihrem Programm ab, bis etwa 135 000 Mark zusammengekommen waren. Sie führten dies als Beweis dafür an, daß Btx keine Systemsicherheit gewährleiste.

Die Post reagierte prompt, gestand den Softwarefehler ein und versprach Abhilfe. Der Softwarefehler wurde schnellstens behoben. Inzwischen sind aber an der CCC-Version Zweifel aufgekommen. Zwar sei es möglich, daß der Fehler auftrete, doch könnten auf keinen Fall gleichzeitig beide Kennungsteile auf dem Schirm erscheinen, wie die Hacker behaupten. Vielmehr geht man in Bonn davon aus, daß Kennwortteile des Haspa-Anschlusses auf andere Weise bekannt wurden – etwa durch unzureichende Geheimhaltung bei einer öffentlichen Vorführung. Eine dritte Möglichkeit kommt noch in Betracht: die Hakker könnten ihre Kenntnisse auch aus dem Arbeitsrechner einer Vermittlungsstelle bezogen haben, in dem teilnehmerbezogene Daten kurzfristig gespeichert waren. Das Wort „Bankraub", das der CCC bei seiner Darstellung der Vorgänge verwendete, ist irreführend. Denn ein Einstieg in einen bankeigenen Rechner und damit der Zugriff auf Geld und Konten ist über die beschriebene Methode unmöglich. Obendrein hatte die Haspa zu diesem Moment ihren externen Rechner noch nicht ans System angeschlossen.

Daß der CCC die 135 000 Mark erhalten hätte, wenn er nicht darauf verzichtet hätte, ist unwahrscheinlich. Laut § 13 der Fernmelde-Ordnung werden zu Unrecht erhobene Vergütungen zurückerstattet. Wenn einem Nutzer die Kostenrechnung zu hoch erscheint, erklärt er, daß er nicht zu zahlen bereit ist. Der Anbieter muß dann auf dem Rechtsweg nachweisen, daß er die Vergütungen zu Recht beansprucht.

Da der Hamburger Vorfall offenbar aufgrund eines freizügig geschalteten Anschlusses möglich wurde, fordert die Post Btx-Nutzer auf, nur dann ihren Anschluß freizügig zu schalten, wenn dies unumgänglich ist. Bei der Handhabung der Kennzahlen und Paßwörter sei größtmögliche Geheimhaltung erforderlich, um das Risiko zu mindern, daß Unberechtigte davon Kenntnis erhalten. Im Lauf des nächsten Jahres soll der Nutzer schon auf der Begrüßungsseite auf die Freizügigkeit seines Anschlusses hingewiesen werden.