Durch die Hintertüre ins System

Wie sicher sind Ihre Daten in Btx?

Wie sicher sind die Datenbestände von Computer-Systemen vor unbefugtem Zugriff? In den USA werden immer häufiger Schwachstellen durch jugendliche EDV-Freaks aufgedeckt: Mit Hilfe des eigenen Heimcomputers schleichen sie sich in die Datennetze von Großfirmen. Sogar schon Rechner des Pentagon wurden von ihnen angezapft. Bange Frage: Wird Mißbrauch auch beim künftigen Massenkommunikations-Medium Bildschirmtext an der Tagesordnung sein?

Eine Art neuen amerikanischen Nationalsports für jugendliche Computer-Fummler: Mit ihrem Heim-Computer schaffen immer mehr via Telefonleitung den Einstieg in Rechneranlagen nicht nur von Privatfirmen, Banken, und Forschungsinstituten, sondern selbst in die Datenbanken des US-Verteidigungsministeriums (siehe auch Kasten „FBI"). Die sogenannten „Hacker" haben im allgemeinen leichtes Spiel: Über „Telenet", einem kommerziellen Datenverbund mit über 1200 angeschlossenen externen Rechnern, gelingt der unbefugte Einstieg fast ohne große Mühe. Die Berechtigungsnummern für die Nutzung von „Telenet" bestehen – ähnlich Bildschirmtext – aus siebenstelligen Zahlen- und Buchstabenreihen. Und die sind durchaus zu knacken.

Durch „Hacker" ist bereits Schaden in Millionenhöhe entstanden. Sie zapfen nicht nur die aufgestöberten Datenbanken an, sondern manipulieren dort abgelegte Informationen, bringen sie durcheinander oder vernichten sogar gespeicherte Bestände.

Eine erschreckende Fiktion ist jüngst publikumswirksam in den Lichtspielhäusern angelaufen: Der Hollywood-Film „Waregames" (Kriegsspiele). Hier schafft es ein Pennäler, sich auf der Suche nach spannenden Computerspielen bis in den Zentralrechner des Pentagon einzuhacken. „Weltweiter nuklearer Krieg" heißt dann diese makabre Partie. Auf den großen

Aus dem Spiel wird Ernst

Bildschirmen in der unterirdischen Kommandozentrale wird der Atomschlag simuliert; Russische Raketen beim Anflug auf amerikanische Städte. Aus dem Spiel droht bitterer Ernst zu werden. Der Angriff setzt automatisch Gegenreaktionen der Verteidiger in Gang. Die Welt befindet sich am atomaren Abgrund. Daß es dann doch noch ein Happy-End gibt, läßt die Story kaum erträglicher erscheinen.

Als einen der Hauptgründe, weshalb sich so viele „Hacker" in fremde Datenbanken einschleichen können, nennen Computerfachleute die teilweise völlig unzureichenden Sicherheitsschranken. Kein bestehendes Computersystem kann ja

Fortsetzung auf Seite 22

Angstvision aus dem Film „Waregames": Ein Schüler „hackt" sich in den Zentralrechner des Pentagon.

FBI: Jugendliche knacken Computer

Was in Deutschland in den Kinos noch als Zukunftsvision läuft, scheint in den USA bereits Wirklichkeit zu werden: Die amerikanische Bundespolizei (FBI) hat bei Razzien Beweise gefunden, daß Teenager-Banden mit Computer-Manipulationen die Zentral-Computer des Atomforschungszentrums in Los Alamos, der Luftwaffenbasis bei Sacramento und des Forschungsinstituts von Massachusetts angezapft haben. Wie der Sprecher der ermittelnden Abteilung, James Mull, unlängst in Alexandria/Virginia erklärte, werde es noch Monate dauern, bis der gesamte Sachverhalt aufgeklärt ist. Schon heute lasse sich jedoch absehen, daß die System-Manipulationen einen Schaden von mehreren hunderttausend Dollar verursacht hätten.

Bei Hausdurchsuchungen fand die Polizei in dieser Woche nach Angaben des Sprechers bei Teenagern in Rochester, Los Angeles, Detroit, Oklahoma City und anderen Städten Computer, Telefoneinrichtungen und wichtige Aufzeichnungen. Es gebe noch keine Verhaftungen, doch bestehe der Verdacht auf Betrug und unerlaubte Benutzung von Telefon- und Computereinrichtungen. Die Untersuchungen wurden ausgelöst, nachdem die eine Firma, die über 1200 kommerzielle Computereinrichtungen betreut, nichtidentifizierbare Unterbrechungen entdeckt hatte. Bereits im Juli hatte die Polizei eine Jugendgruppe aufgespürt, die das Rechenzentrum einer Lebensmittelkette in Manhattan/New York angezapft hatte. Aus Milwaukee meldet die Polizei eine Bande, die über 60 Rechenzentren, einschließlich Verteidigungseinrichtungen erreicht hat. In keinem der Fälle waren die Betroffenen bisher mit dem Gesetz in Konflikt geraten. *(ddp)*

Durch die Hintertüre ins System

vollkommen sicher sein. Vor allem aber gelten jene Systeme als gefährdet, die wie das amerikanische „Telenet" oder Bildschirmtext besonders benutzerfreundlich angelegt sind.

Als sicherste Methode für den Schutz von Daten vor unbefugtem Zugriff gilt beispielsweise der ständige Wechsel von Paßwörtern. Bei Überweisungen oder Abbuchungen vom eigenen Telekonto etwa, muß der Teilnehmer sogar für jeden einzelnen Vorgang eine elfstellige Transaktionsnummer eingeben – jedes mal eine neue. Bei vielen anderen interaktiven Anwendungen sind derartige Sicherungen weniger aufwendig, um den Teilnehmern die System-Handhabung so einfach wie möglich zu machen. Durchaus ist es deshalb vorstellbar, daß Btx-„Hakker" fremde Kundennummern bei Großversandhäusern ausfindig machen und dann über diese Nummern und mit falschem Namen Bestellungen in Auftrag geben könnten. Je mehr Kunden ihren Wareneinkauf in Zukunft über Btx abwickeln, desto größer wird die Wahrscheinlichkeit, daß eine der neunstelligen Kundennummern per illegal gelenktem Zufall erwischt wird. Selbst wenn aus solchem Betrug keinerlei Gewinn erwachsen kann: Denn letztlich ist ein Kaufvertrag (auch über Btx) ja erst dann perfekt, wenn der Kunde die Warensendung bei der Auslieferung akzeptiert. Und das wird er wohl schwerlich tun, wenn der Bestellvorgang gar nicht von ihm selbst getätigt wurde.

Filmbeispiel „Waregames": Unruhe in der US-Kommandozentrale. Der „Hacker" ist in die geheime Datenbank eingedrungen.

Betrug – aber ohne Gewinn

Inwieweit derartiges bereits während der Feldversuche vorgekommen ist, darüber halten sich die Sprecher der großen, in Bildschirmtext vertretenen Versandhausanbieter verständlicherweise bedeckt. Sie wollen auf die Möglichkeit des Mißbrauchs nicht auch noch ausdrücklich hinweisen.

Laut Artikel 14/7 des Btx-Staatsvertrages begeht jeder eine Ordnungswidrigkeit, „der unbefugt Angebote oder Einzelmitteilungen unter dem Namen eines anderen Anbieters oder Teilnehmers in das Btx-System eingibt oder aus ihm abruft". Schon der Btx-Einstieg mit illegaler Identifizierung ist also keineswegs ein Kavaliersdelikt und kann mit einer Geldbuße bis zu 50 000 Mark geahndet werden – „soweit die Handlung nicht in anderen Vorschriften mit Strafe bedroht ist". Dies ist zweifelsohne dann der Fall, wenn unter dem Namen eines anderen Btx-Teilnehmers versucht wird, Waren zu bestellen, Reisen zu buchen oder gar fremde Konten zu plündern.

Die Belange des Datenschutzes hält beispielsweise der Berliner Rechtsanwalt Jens Peter Lachmann (siehe rechts) für weit „über das hinausgehend, was für alle anderen Kommunikationsmedien gilt". Wie sieht es aber technisch aus? Könnten theoretisch fremde Konten angezapft werden? Der „König der Hacker", der Amerikaner Richard Cheshire, verneint dies in einem Interview mit dem Nachrichtenmagazin „Der Spiegel". So sei das amerikanische Telefonnetz ganz anders aufgebaut als das deutsche. Und deshalb würde in der Bundesrepublik würde das Anzapfen von externen Rechnern kaum in dem Umfang gelingen wie es in den USA an der Tagesordnung ist. Gewissermaßen ein Lichtblick.

Kein Sündenbock für Probleme

Ist Btx ein sicheres System? Der Bundesbeauftragte für den Datenschutz, Reinhold Baumann ist nicht dieser Ansicht: Für ihn bleiben Zweifel, ob die in das System implementierte Sicherheit genügt (siehe Kasten links). Der Wissenschaftler Jürgen Seetzen vom Berliner Heinrich-Hertz-Institut hingegen meint, daß Btx „kein Sündenbock für Probleme sein darf, mit denen wir seit geraumer Zeit generell leben müssen". Seetzen: „Natürlich ist es nicht auszuschließen, daß bei Btx Überraschungen mit neuen Dimensionen auftreten können. Überraschungen aber sind nicht prognostizierbar und ich gehe davon aus, daß sie bei Btx beherrschbar bleiben."

Gerhard Breinlinger

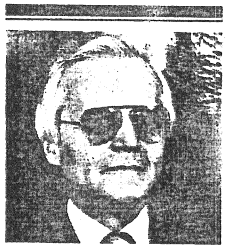
Was meint der Bundesdatenschutzbeauftragte?

Es bleiben Zweifel

„Der Bundesdatenschutzbeauftragte Dr. Reinhold Baumann geht davon aus, daß die Deutsche Bundespost die bisherigen Feldversuche auch unter dem Aspekt, der Sicherheit für Teilnehmer und Anbieter ausgewertet hat: Mir sind die Ergebnisse im einzelnen nicht bekannt. Deshalb bleiben Zweifel, ob die im System implementierte Sicherheit in allen Punkten den Forderungen des Bundesdatenschutzes genügt. Insbesondere habe ich den Eindruck, daß es noch zu leicht möglich ist, daß sich ein Teilnehmer unter falscher Identität Zugang zum System verschafft. Dieses Problem hat besondere Bedeutung auch vor dem Hintergrund der systembedingt nur begrenzten Sicherheit des Fernsprech-Wählnetzes. Zu dem erst kürzlich aufgenommenen Wirkbetrieb erwarte ich derzeit noch technische Informationen vom Postministerium.

○ Soweit gegenüber dem ‚normalen' Seitenabruf zusätzliche Sicherheiten (z. B. Persönliche Kennwörter und Transaktionsnummern) bestehen, erscheint die Sicherheit aus der Sicht des Datenschutzes ausreichend.

○ Solange der Btx-Systemzugang nicht besser gesichert ist, halte ich im Anbieterrechner zu realisierende zusätzliche Schutzmaßnahmen für erforderlich.



Dr. Reinhold Baumann

○ Hinsichtlich der geschlossenen Benutzergruppe verweise ich auf meine Äußerung zur Systemsicherheit generell: Wer unter der Kennung eines Fremden in das System eindringt, erlangt auch dessen Zutrittsrechte in geschlossene Benutzergruppen.

Aus dem gleichen Grund sollten Inhouse-Systeme zusätzliche Sicherungen beinhalten.

○ Die Datenschutzregelungen im Staatsvertrag entsprechen im wesentlichen den schon früher erhobenen Forderungen. Unbefriedigend ist meines Erachtens die Regelung des Abrechnungsverfahrens. Hier hätte ich ein striktes Verbot der Registrierung von Art und Inhalt in Anspruch genommener Angebote vorgezogen. Außerdem halte ich eine gesetzgeberische Entscheidung für notwendig, inwieweit gesetzliche Durchbrechungen des Fernmeldegeheimnisses (z. B. Gesetz zu Art. 10 GG) auch für Btx gelten.

○ Technisch wäre es möglich, durch Registrierung des Kommunikationsverhaltens der Teilnehmer Persönlichkeitsprofile zu erstellen. Die Datenschutzvorschriften sollen sicherstellen, daß aus dieser Kontrollierbarkeit keine Kontrolle wird. Darauf zu achten ist auch Aufgabe der Datenschutzbeauftragten in Bund und Ländern."