taz Samstag, 22.12. 84

0200

Wie der Btx-Code der Hamburger Sparkasse geknackt wurde

Bildschirmtext im Schwachstellentest

Seit dem Coup des Chaos Computer Club Hamburg, durch einen Fehler im Bildschirmtext-System die Hamburger Sparkasse mit knapp 135.000 DM zu belasten, ist Bildschirmtext, kurz: Btx, ins Gerede gekommen und die Chaoten des Chaosclub in die Schlagzeilen.

Bildschirmtext ist eine gigantische Verbraucherverarschung. Über sieben Jahre liefen in Berlin und Düsseldorf «Feldversuche«. Von vornherein war klar, daß das System nach den Feldversuchen eingeführt wird, ganz gleich, wie die »Versuche« ausgehen würden. Die politische Zielsetzung ermöglichte immense Investitionen und machte einen Ausstieg einfach unmöglich. Nach dem »Versuch« konnten die Versuchsteilnehmer ihre Geräte wegwerfen, da sie inzwischen technisch überholt waren. Die Post spendierte, finanziert mit den Telefongroschen, allen Teilnehmern einen 1.000-Mark Gutschein für die technische Umstellung. Doch rund jeder sechste verzichtete auf dieses verlockende Angebot und hörte mit Btx auf. Die Post prophezeite für Ende 1984 150.000 Teilnehmer. Es waren müde 20.000. Unter denen sind viele keine aktiven Teilnehmer. Inzwischen verzichtet die Post auf eigene Prognosen und gibt ein paar Millionen aus für Programme, die - unter anderem - bessere Vorhersagen machen sollen.

Die Post hat in Btx mehr als 700 Millionen investiert. Vergleicht man das mit Subventionen für Opernhäuser, so hat die Post jedem Teilnehmer eine Loge für 35.000 Mark gezimmert. Nur das Opernprogramm ist noch recht eintönig.

IBM ist der Lieferant des Computers und der Programme für das laufende System. Die haben sich ein gutes Geschäft versprochen und wollten ihr System an verschiedene Länder verkaufen. Immerhin haben bisher umgefähr 100 Leute rund zwei Jahre herumprogrammiert. Wenn man für einen dieser Spezialisten mal 20 000 Mark Kosten im Monat ansetzt, gibt das rund 50 Millionen. Mehrere Manager wechselten sich in der Betreuung des Projektes ab. Immer nur »Kleinigkeiten« im Programm mußten noch verbessert werden und bei Programmen dauern Korrekturen um so länger, je kleiner sie sind.

Chaos-Team wird Btx-Anbieter

Im Herbst 84 entschloß sich der Chaos Computer Club nach langen Debatten, an Btx teilzunehmen. Natürlich als »Anbieter«, Teilnehmerdasein ist uninteressant. Begonnen wurde mit dem billigsten Gerät, das technisch aufgefrischt wurde. Doch die ersten Monate wurden zur Qual. Bei Heimcomputern kennt man ja die Grundstimmung: »Einschalten - Geht nicht«. Aber von der Post erwartet jeder, daß alles funktioniert. Nur selten aber kommt Post von der Post mit dem Text »Wegen Arbeiten am System kann am Wochenende kaum telefoniert werden«. Bei Bildschirmtext klappte kaum etwas. Schon ein Akzent am Buchstaben im Namen bringt ungeahnte Verwicklungen (und das bei einem »europäischen« System). Angesichts der Computerisierung bieten sich Namensänderungen mit Akzenten als subversive Strategie an. Außerdem klappte das Sperren und Entsperren von Seiten nicht. Gesperrte Seiten waren lesbar, entsperrte nicht. Die Post sagte denen, die sich beschwerten: Ihr macht was verkehrt. Gesperrte Seiten sind sowas wie die geschlossenen Türchen beim Adventskalender. Am ersten Dezember wird das erste Türchen aufgemacht (bei Btx: entsperrt), am zweiten das zweite usw. Die Post hat ein Weihnachtskalender-Gewinnspiel in Bildschirmtext. Jeden Tag können neue Buchstaben hinter einem Türchen angeschaut werden und am 24.12. gibt es einen vollständigen Satz (sinnige Glückwünsche von der Post). Ganz ohne Brecheisen gingen aber schon am Monatsanfang alle Türchen auf. Entweder hat sich jemand bei der Post vertippt oder das System hat noch einen kleinen Fehler. Der Chaos Computer Club (CCC) hat das erst am 12. Dezember mitbekommen und den vollständigen Lösungssatz eingeschickt. Es gibt Telefoneinheiten zu gewinnen. Interessant ist, wieviel Teilnehmer vor dem CCC die Lösung einschickten. Ob die Post auch hier behauptet, irgendwelche Chaoten hätten die Lösung bei der Post ausgespäht?

Ein Hauptproblem bei Btx ist aber das Erstellen von Seiten. Der CCC macht eine Art elektronische Zeitung, deren Erscheinungsweise unregelmäßig ist. Wenn ein neuer Artikel geschrieben ist und im System abgeladen werden soll, fokussieren sich die Blicke auf die unterste Zeile und warten auf die Meldung »ED007 - DURCHFUEHRUNG ZUR ZEIT NICHT MOEGLICH« oder andere »Geht grad nicht«.

Um in das Btx-System einzudringen, ist es lediglich erforderlich, die Anschlußkennung zu wissen. Jeder Teilnehmer hat eine andere zwölfstellige Ziffer. Diese Zugangsberechtigung wird in der Regel durch einen Knopfdruck geschickt. Das ist praktisch und recht sicher. Man kann sich das so vorstellen wie ein neunstelliges Zahlenschloß (die ersten drei Ziffern sind meist Null) am eigenen Fahrradkeller. Zum zweiten gibt es ein persönliches Kennwort. Das ist vergleichbar mit einem Zahlenschloß am Fahrrad. Und dann kann man sein Fahrrad auch in einen Gemeinschaftskeller stellen. Bei Btx heißt das »Freizügig schalten«. Dann kann jeder in den Gemeinschaftskeller gehen und, wenn er eine Nummer eines bestimmten Fahrradschlosses kennt, damit durch Btx reisen und sich irgendwas anschauen. Vieles ist umsonst, manche Informationen oder Angebote kosten etwas. Springermeldungen kosten 1 Pfennig, FAZ-Meldungen 2 Pfennig und dafür zahlt der Fahrradbesitzer, nicht der Fahrer.

→

Btx-Schwachstellentest

Irgendwann diskutierte man beim CCC wieder über Btx und die Politik der Post, die Risiken von Btx einfach zu verschweigen und zu leugnen. Dabei tauchte die Frage auf, ob das Absicht oder Dummheit ist. Man beschloß einen Test. Wer kam als Versuchskaninchen in Frage? Das Bundespostministerium in Bonn? Da reicht ein Zitat. In einem Leserbrief der Pressestelle stand sinngemäß : Btx sei sicher, weil die Telefonleitungen schwer anzapfbar seien, da sie hierzulande unterirdisch liegen.

Die Ulmer Leitzentrale von Btx ist als Versuchsobjekt nicht so interessant. Sie versucht, das System am Laufen zu halten. Und die Berliner sind bei Btx dafür zuständig, Postkunden zu beruhigen, wenn mal wieder was nicht geht. Das Fernmeldetechnische Zentralamt (FTZ) in Darmstadt ist die Stelle, die technische Konzepte und Normen erstellt. Dort sitzen so erwartet man, die Praktiker, die die Sicherungskonzepte ausgearbeitet haben. Das sind die richtigen Leute für einen Btx-Schwachstellentest. Ohne sich das genauer überlegt zu haben, wurde vom CCC eines Tages der Btx-Anschluß des FTZ getestet: Haben die freizügig geschaltet oder nicht? Um das rauszukriegen, mußte erst deren Teilnehmernummer getippt werden: 06151 83. Das ist die Telefonnummer des FTZ. Dann kommt die Abfrage des geheimen Kennworts. Man kann da irgendwas tippen und an der anschließenden Fehlermeldung erkennen, ob das FTZ freizügig geschaltet hat oder nicht. Der CCC tippte irgendwas: dieselbe Telefonnummer nochmal. Das FTZ war unvorsichtig: der Anschluß war freizügig geschaltet. Es kam aber noch dikker: Das FTZ hatten die eigene Telefonnummer als geheimes Kennwort ausgesucht. Das ist entschieden unvorsichtiger, als man es zumindestens von Fachleuten der Post erwarten durfte.

Beim Hamburgischen Datenschutzbeauftragten wird Buch geführt, wer wann an Btx gearbeitet hat. Da das Btx-System meldet, wann zuletzt jemand »dran« war, läßt sich so eine »Fremdbenutzung« oft feststellen. Aber kaum jemand sonst führt darüber Buch, es ist umständlich. Das FTZ merkte die »Fremdbenutzung« durch den CCC jedenfalls nicht. Damit war die Frage geklärt: Die Post informiert aus Dummheit nicht bzw. falsch über Btx.

Der CCC überlegte, was nun zu tun sei. Die naheliegendste Sache war natürlich, sich bei der Post Geld zu holen. Dazu wird eine gebührenpflichtige Seite eines anderen Btx-Teilnehmers aufgerufen. Und das läßt sich beliebig oft wiederholen. Der höchste Preis einer Seite ist gegenwärtig DM 9,99. Mit 1-Pfennig Seiten von Axel Springer testete der CCC auf eigene Kosten, wie schnell sich so Geld sammeln läßt. Es ergab sich im nicht-automatischen Betrieb ein Wert von rund 10 DM pro Stunde. Bei der Spendenseite des CCC für 9,97 wären das also rund 10 000 DM pro Stunde. So über Nacht kommt da schon was zusammen. Diese Gebühren werden mit der Telefonrechnung - in dem Fall also der Telefonrechnung des FTZ - erhoben und ein paar Wochen später den Anbietern überwiesen. Es klappt zwar zur Zeit mal wieder nicht, die Post hat da einen Fehler im Programm, sie hofft, im Februar die Gebühren zahlen zu können. Grundsätzlich wird das Geld jedenfalls verbucht.

Das Holen des Geldes wäre die Phase eins. Was dann? Sollte man der Post diese Sicherheitslücke verkaufen? Man hätte ja, wie es in der Industrie üblich ist, so 100 000 Mark oder mehr darauf »hacken« können und der Post für einen bestimmten Prozentsatz des Geldes Beratung zu diesem Problem verkaufen können. Oder lebenslänglich umsonst telefonieren für den CCC oder ähnliches. Wegen offenkundig grober Fahrlässigkeit müßte die Post zahlen.

Der Preis wäre allerdings in beiden Fällen Stillschweigen gewesen. Andernfalls wäre die konzentrierte Wut der Postoberen zu erwarten. In der Folge hätte vielleicht ein halbes Dutzend Behörden versucht, etwas gegen den CCC zu machen.

Der CCC wollte aber Aufklärung über die Risiken dieser neuen Systeme. Dazu mußte die Finanztransaktion öffentlich vorgeführt werden. Gut, aber wer sollte auf den Startknopf für den Geldtransfer drücken? Das ist immerhin eine Ordnungswidrigkeit wie falschparken, aber etwas teurer; bis 50.000 DM Bußgeld. Macht's der Datenschutzbeauftragte? Wahrscheinlich hätte er die Möglichkeit zur Kenntnis genommen und versucht, auf dem Dienstwege eine Verbesserung zu erreichen.

Ein Politiker? Vielleicht. Aber wenn er's verpetzt? Blieb eine Möglichkeit: Selber machen und die Strafbarkeit durch die öffentliche Darstellung aufheben. Über eine Woche später schlug der Versuch fehl, da das FTZ seinen Anschluß inzwischen nicht mehr freizügig geschaltet hatte.

Hacker als Datenschutzfachmann

Einige Wochen später hielt Wau einen Vortrag auf einer Datenschutzfachtagung in Köln: Btx - Eldorado für Hacker. In Köln lief alles im Nadelstreifen herum. Wau wirkte wie ein Papagei dazwischen. Trotz anfänglicher Distanz war das Publikum vom Vortrag beeindruckt. Nur der Vertreter der Post meinte, das sei unter der Gürtellinie und dazu wolle er nichts sagen. Das wurde mit Lachen quittiert. Denn im Vortrag wurden eine Reihe von Fehlern drastisch und plastisch geschildert. Ein Fehler liegt im Versand elektronischer Briefe. Der Absender kann den Inhalt noch ändern, nachdem der Brief angekommen ist. Man kann einem Geschäftspartner ein Angebot über sagen wir 2.300 DM schicken und nachträglich den Preis ändern; je nachdem erhöhen oder verringern. Ein anderer Fehler bewirkte, daß das Btx-System unter bestimmten Umständen interne Systeminformationen ausspuckte. Mit etwas Glück könnten so auch Anschlußkennungen und die geheimen Kennwörter bekannt werden. »Unfug« meinte der Postvertreter dazu. Und auf das Angebot der Kooperation kam nur die Antwort »Da müssen Sie erst seriöser werden«. Es ist unklar, ob das dem CCC gelungen ist. Zumindest spuckte das Btx-System nach etlichen Versuchen mit dem bekannten Systemfehler Anschlußkennung und Kennwort der Hamburger Sparkasse aus. Damit war es möglich, die für das FTZ geplante Vorführung mit der Sparkasse durchzuführen.

Es ging fast alles wie geplant. Über Nacht kamen in 12 Stunden und 59 Minuten gut 134.000 Mark zusammen. Mit einem tragbaren Kleincomputer wurden die gebührenpflichtigen Seiten im Dreisekundentakt automatisch abgerufen. Anschließend machte der CCC klar, daß der Coup am 19.11. morgens um 8 Uhr der Presse und dem Fernsehen in den Räumen des Hamburgischen Datenschutzbeauftragten vorgestellt werden sollte. Übrigens hatte Dr. Christian Schwarz-Schilling an dem Tag Geburtstag.

Die Post gab den Fehler zu, er war ihr »peinlich«. »Viereinhalb Monate Betrieb und der erste Fehler« verlautete von der Post in Hamburg. Sie schaffte es in der Rekordzeit von zwei Tagen, ihn (soweit bekannt) zu beheben. Die Banken waren erstaunt. Und in der nächsten Ausgabe der »Computerwoche«, einer Fachzeitung für gehobene Datenverarbeitung, hieß es lapidar »Wer ... sich in den kommenden zwei bis drei Jahren dem Btx-System anschließt, gehört wegen Dummheit bestraft«.

Damit ist die Geschichte aber noch nicht zu Ende. Der Haken, an dem die Post hängt, heißt Haftungsrisiko. Wenn ihr System so einen Unfug gestattet, haftet sie. Und das paßt ihr nicht. Nach einer Woche versuchte die Post, ihren Kopf aus der Schlinge zu ziehen. Sie unterstellte dem CCC, er habe das Kennwort nicht durch den Systemfehler erhalten, sondern durch »Ausspähung«. Da Hacker aber faul sind und das Kennwort vom FTZ schon aus Versehen kriegen, ist klar, daß das eine Schutzbehauptung der Post ist. Die Sparkasse sieht das ähnlich. Damit ist die Geschichte für den CCC zu Ende. Er hat wichtigeres zu tun als Fehler im Bildschirmtext zu suchen. Die beste Lösung beim System hieße zwar: Ausschalten und abschreiben. Aber das ist politisch nicht gewollt von denen, die am Drücker sitzen. Vielleicht ist das aber ein Anlaß, endlich die 20 roten Warnseiten über Btx zu gestalten.

wau

Treffen für Datenreisende:
Chaos Communication Congress '84 am 27./28.12., Eidelstedter Bürgerhaus, Elbgaustr.12, 2000 Hamburg 54. Kontakt: ☎040 - 570 38 12

Praktischer Hinweis

Die Datenverarbeitung zieht still und leise in unser aller Alltag ein. Es ist schwer, sich dagegen zu wehren. Ein paar praktische Hinweise: - Gib nie Daten ab, wenn es Dir nicht unmittelbar einleuchtet. Selbst dann sei vorsichtig. Fragen kostet nichts, Zeit muß dafür vorhanden sein. - Mache bei Deinen Daten klar, daß sie höchst persönlich sind und erkundige Dich, wie die datenfordernde Stelle Datenschutz handhabt. Kündige Deine Abbuchungsaufträge. Bedenke, was ein einzelner Programmierer bei den Elektrizitätswerken anrichten kann mit ein paar Millionen automatischen Einziehungsaufträgen. - Laß Dich nicht verkabeln. Halte Deine Daten selbst in Ordnung und überlasse es nicht anderen, auch wenn es bequemer ist.

wau