



Am 17.11.1984 wurde in den Räumen des Hamburgischen Datenschutzbeauftragten eine Möglichkeit des Btx-Bankraubes auf Knopfdruck gezeigt. Die betroffene >Hamburger Sparkasse< fand eine Abrechnung über Bildschirmtextteilnehmergebühren in Höhe von rund 135 000 DM vor. Der Begünstigte - der Chaos Computer Club - erhebt jedoch keinen Anspruch auf das Geld; die Aktion sollte lediglich die bei Btx vorhandenen Mängel öffentlich darstellen.

Es ist kein Kundenkonto davon betroffen, sondern nur die Fernmelderechnung der >Hamburger Sparkasse< als einfacher Btx-Teilnehmer.

Durch einen Systemfehler in Bildschirmtext (Überlauf bei Decoder-Seiten) wurde deren geheime Btx-Zugangskennung auf einer neu erstellten Seite angezeigt. Mit dieser Kennung wurde anwesenden Vertretern verschiedener Medien praktisch gezeigt, wie auf Knopfdruck jeweils 9,97 DM durch Aufruf einer gebührenpflichtigen Seite von der Sparkasse zum Chaos Computer Club transferiert wurden.

Der Aufruf der gebührenpflichtigen Seite wurde durch einen Kleinrechner mit maximaler Geschwindigkeit gesteuert, damit nur der gebührenpflichtige Aufruf erfolgte und eine Anzeige der Seite nicht möglich war.

Nach der gegenwärtigen Rechtslage trägt der gewöhnliche Btx-Teilnehmer als Verbraucher das Haftungsrisiko in derartigen Fällen; daß es sich beim Btx-Teilnehmer gerade um eine Sparkasse handelt, spielt keine Rolle. Sie müßte zahlen, wenn nicht auf das Entgelt verzichtet worden wäre. Grundsätzlich wurden diese Probleme in der >datenschleuder 3< und am 15.11.84 auf der 8. DAFTA (Datenschutzfachtagung) erläutert.

Daraufhin gab es Einwände aus Postkreisen, das sei praktisch unmöglich. Um darzustellen, welche Probleme im Btx-System stecken, hätte es genügt, einen Pfennig umzubuchen. Aber wie groß die Gefahr für jeden einzelnen Btx-Teilnehmer wirklich ist, konnte nur so praktisch gezeigt werden. Zudem zeigte sich die Post uns gegenüber erst dann kooperationsbereit, wenn wir ihr Fehler nachwiesen; Fehlermeldungen und Anfragen zeigten wenig Reaktion.

Auf der 8. DAFTA erklärte Wau Holland, daß das Btx-System unter bestimmten praktischen Bedingungen interne Informationen ausspuckt. In der Regel wird von Anbietern beim Btx-System der Platz auf den einzelnen Informationsseiten nur zum Teil genutzt. Wenn aber eine Decoderinformation mit exakt soviel Zeichen gefüllt wird, wie die Post erlaubt, schickt das Btx-System aufgrund eines Fehlers dem Teilnehmer irgendwelche Daten zusätzlich.

In einem Fall war es die Kennung der Hamburger Sparkasse.

In einem anderen Fall war es nur Name und Systemnummer eines Teilnehmers aus Hessen. Dieser Effekt kann auf Seite 6665552222 angeschaut werden.

Da es bislang nicht vorhersehbar ist, welche Daten das Btx-System bei dieser Überlaufbedingung offenbart und somit jeder Teilnehmer davon betroffen sein kann, stellt der Fehler Btx grundsätzlich in Frage. Man könnte der Post wegen dieses Systemverhaltens Fahrlässigkeit vorwerfen. Wer trägt dann das Risiko?

Zu diesen verblüffenden Mängeln beim Bildschirmtextsystem kommt noch die Unkenntnis vieler Menschen hier zum Thema Datensicherheit hinzu.

Die Post verlangt von allen Teilnehmern des Bildschirmtextdienstes, daß sie die Risiken kennen und macht den Einzelnen für alle Vorgänge, die unter seiner Anschlußkennung geschehen, verantwortlich.

Das ist nicht realistisch.

Für die meisten Btx-Teilnehmer sind die Sicherheitsfragen einfach unklar. Soweit uns bekannt führen gerade die Datenschutzbeauftragten Buch über die Anschlußzeiten, um Zugriff Dritter festzustellen. Selbst die Datenverarbeitungsfachleute der Post tun das selten; in den Telefonläden geschieht das in der Regel nicht. Die >fachkundige Beratung< dort ist in erster Linie aufs Verkaufen ausgerichtet; die Mißbrauchsgefahren sind in der Regel unbekannt oder werden verschwiegen.

Angesichts der jetzt bekannten Fehler gibt es bei Btx nur zwei Möglichkeiten: ganz abschalten oder Verbot aller Finanztransaktionen.