Organisatorische, technische und juristische Schutzmöglichkeiten machen Bildschirmtext fast „einbruchsicher"

# Sechs Richtige wahrscheinlicher als Hacker-Einstieg in Btx

**Juristen und Techniker müssen, wenn sie das Problem Datenschutz und Datensicherung in den Griff bekommen wollen, Hand in Hand arbeiten — speziell beim relativ neuen Postdienst Bildschirmtext. Aber immernoch wird zu viel zu emotional und ohne hinreichende Sachkenntnis miteinander diskutiert. Gefahren gibt es in der Tat überall, „aber es gilt sie zu relativieren", empfiehlt Wolfgang Gorn, Autor des folgenden Artikels. Er beruhigt: „Man kann sich ausrechnen, daß ein unberechtigtes Eindringen ins Btx-System eine geringere Wahrscheinlichkeit hat als sechs Richtige im Lotto". Auch biete das Bundesdatenschutzgesetz (BDSG) schon seit Jahren — im internationalen Vergleich — nicht gerade unbedeutenden Schutz. Hacker in der Bundesrepublik dürften innerhalb des Btx-Systems wenig Chancen haben — allerdings unter der ganz wichtigen Voraussetzung, daß alle Schutzmöglichkeiten, die es organisatorisch, technisch und juristisch schon gibt, auch intensiv genutzt werden.**

Btx ist technisch gesehen Fernmeldedienst und EDV-Peripherie. Damit unterliegt Btx eindeutig dem BDSG und dem Fernmelderecht. Leider haben sich alle Parteien und die vorige Bundesregierung nicht ausreichend um die rechtliche Seite von Btx gekümmert, und so konnten die Bundesländer eine vermeintliche Gesetzeslücke ausfüllen (wozu sie grundsätzlich gemäß Grundgesetz berechtigt sind). Dazu kommt, daß Bildschirmtext von den Bundesländern gegen alle Bedenken der Fachleute als „Neues Medium" definiert wurde, wofür — entsprechend der Kulturhoheit der Länder, aber auch hier schon unsinnig — Landesrecht zuständig ist.

Auf diese Weise haben wir heute neben dem Bundesdatenschutzgesetz (BDSG) und dem Fernmelderecht — hier insbesondere die Fernmeldeordnung (FO), auch noch den Staatsvertrag der Bundesländer zu Btx (BtxStV) zu beachten.

## „lex specialis"

Es gilt als „lex specialis" neben allen anderen Gesetzen und Verordnungen, wenn auch viele ernsthafte Fachleute — Juristen und Techniker — seine Daseinsberechtigung aus vielen guten Gründen anzweifeln. Dies gilt besonders für die Bestimmungen des Artikel 9 zum Datenschutz und auch für die unklaren Formulierungen des Artikel 8 zur Werbung, der mehr Unsicherheit schafft, als klärend wirkt.

Btx wird im Staatsvertrag einerseits technisch eingeengt (Ausschluß der Bewegtbildübertragung, die mit breitbandigen Netzen kommt und viele Vorteile bringen wird) und andererseits so einseitig als „Medium" mit allen Konsequenzen definiert, daß die Kulturhoheit der Länder unabdingbar erscheint. Aber was sind das für Länder, die im Zeitalter der UNO und EG eine solche Hoheit reklamieren, die mehr als antik und unzeitgemäß ist! Hier wird versucht, Bundes- und internationales Recht in einer Weise zu regeln, die diesen Staatsvertrag als rechtspolitisch und rechtssystematisch als unhaltbar abstempelt, wenn er auch zur Zeit als geltendes Recht beachtet werden muß.

Außerdem muß man Dinge da regeln, wo sie hingehören — hier aber wird Datenschutz zum Prügelknaben falsch verstandenen Verbraucherschutzes! Die amtliche Begründung zu Artikel 9 BtxStV — Datenschutz — geht von einem „besonderen Gefährdungspotential" von Btx aus. Es wird hier völlig verkannt, daß Btx nur eine technische Variante moderner Datenfernübertragung (DFU) im Rahmen der Datenverarbeitung (DV) ist. Und hierfür gilt nun einmal das BDSG! Wenn also irgend ein Regelungsdefizit vorliegt, das erst einmal sorgfältig analysiert und definiert werden muß, dann sollte dies im Rahmen einer BDSG-Novellierung geklärt werden.

Das Btx-Netz besteht aus den Btx-Vermittlungsstellen in allen größeren Ortsnetzen, an die die kleineren Orte im Nahbereich angeschlossen sind, aus den Btx-Zentralen zur regionalen Versorgung und der Btx-Leitzentrale in Ulm, die zu den Anbietern und Teilnehmern hin über das öffentliche Telefonnetz — beim Rechnerverbund über Datex-P — und untereinander über internes Postnetz miteinander verbunden sind (Bild 1).

Wir müssen klar sehen, daß einerseits hier die umfangreichste Gefahrenquelle liegt, andererseits Btx aber genau so sicher beziehungsweise unsicher wie das Telefonieren ist. Hier liegt die eigentliche Gefahr der Datenverarbeitung, wie überhaupt die Datenübermittlung sehr kritisch gesehen werden muß. Wenn auch die Kabel in Deutschland überwiegend unterirdisch liegen, so geben Endverteiler und die Verkabelung in Gebäuden genügend Möglichkeiten für kriminelle Aktivitäten mit einfachem technischen Aufwand.

„PIN" und „TAN", die später erläutert werden, bieten Sicherheit gegen

Fortsetzung auf Seite 22

Fortsetzung von Seite 21

# Sechs richtige wahrscheinlicher als . . .

unrechtmäßigen Zugriff auf Datenbanksegmente, bieten gleichsam „elektronische Unterschrift". Die Datenströme selbst sind jedoch nur durch eine End-to-end-Verschlüsselung — also vom Teilnehmer bis in die Datenbank hinein und zurück — gegen Fälschung, Verfälschung oder Mißbrauch zu sichern.

Die Kryptologie bietet zwar viele Möglichkeiten und Geräte, nur ist der Aufwand dafür leider nicht gering und für einen Massendienst zu teuer. Daher werden heute nur besonders sensible geschlossene Benutzergruppen (GBG) damit ausgerüstet. Eine Erweiterung des „Aida"-Verfahrens, das weiter unten erläutert wird (siehe auch CW Nr. 23 vom 1. Juni 84, Seite 22) wäre hier eine sehr gute Hilfe für die DFÜ kleinerer Datenmengen.

## Fernmelderecht und Btx-Technik

In Bild 1 sind die Einrichtungen der Deutschen Bundespost aufgezeichnet, die zur Btx-Versorgung nötig sind. Sie unterliegen alle der Fernmeldehoheit mit dem Fernmelderecht, hier insbesondere der Fernmeldeordnung (FO), sowie dem Strafrecht. Basis hierfür ist Artikel 10 des Grundgesetzes — Brief-, Post- und Fernmeldegeheimnis. Als Ausnahme für die Überwachung gibt es das Grundgesetz 10 und Paragraph 100a StPO bei Verdacht auf schwere Straftaten, wofür jedoch gemäß Paragraph 100b StPO nur ein Richter zur Anordnung der Überwachung zuständig ist.

Die Fernmeldeordnung wurde durch die 22. Änderungsverordnung (ÄndVFO) ergänzt. Für den Datenschutz wurde dabei ein Absatz in den Paragraphen 38b FO eingefügt, der jedoch rein deklaratorische Bedeutung hat, da der Datenschutz hier sowieso Teil des Fernmeldegeheimnisses ist. Rein technisch nötige Daten werden am Ende einer jeden Btx-Nutzung sofort automatisch gelöscht. Bei Btx-Seiten, für die eine Vergütung verlangt wird, werden Teilnehmer- und Anbieternummer, Datum und Uhrzeit (Anfang und Ende) sowie Summe der Vergütung gespeichert, nicht die einzelnen abgerufenen Seiten. Zur Abrechnung mit Teilnehmern und Anbietern werden nur die Vergütungssummen in der Fernmelderechnung ausgedruckt; somit sind die Daten voll anonymisiert. Nur für Revisionsfälle (zum Beispiel das Einklagen von Forderungen) werden die gespeicherten Daten drei Monate im „Ulmer Datensumpf" aufbewahrt und dann automatisch gelöscht.

Somit ist rechtlich und technisch alles getan, um Datenschutz und Datensicherung nach den Regeln des BDSG sicherzustellen.

## Jeder ist „speichernde Stelle"

Unter den Btx-Teilnehmern (Oberbegriff) spielen die Anbieter von Btx-Informationen datenschutzrechtlich eine besondere Rolle. Für sie gelten natürlich erst einmal die Normen des BDSG, darüber hinaus aber auch Artikel 9 BtxStV ff. und damit eine gravierende Erweiterung des Begriffs der „Datei": Das ganze Btx-Angebot wird in Artikel 9 Absatz 5 als Datei definiert! Ob sich die Väter des BtxStV über die Konsequenzen im klaren waren? Jeder Bürger, der am Btx-Mitteilungsdienst teilnimmt, zum Beispiel eine Btx-Seite mit einer Gratulation zum Geburtstag absendet, wird mit zur „speichernden Stelle" (gemäß Paragraph 2 Absatz 3 Ziffer 1 BDSG)!

Die bereichsspezifische Datenschutzregelung des Artikel 9 geht — wie schon erwähnt — von einem „besonderen Gefährdungspotential" aus.

Dies ist unverständlich, da bei einem Btx-Kontakt, soweit der Teilnehmer nur „liest", der Anbieter überhaupt nichts davon erfährt, und — soweit der Teilnehmer zum Beispiel etwas bestellt oder sonstwie eine Willenserklärung von sich gibt — nur die Daten an den Absender geschickt werden, die der Teilnehmer (durch freiwilliges Drücken der Tasten 1 und 9) selbst freigibt. Dabei werden üblicherweise nicht mehr Fakten erhoben als bei einer telefonischen Bestellung oder einer Bestellpostkarte. Wo liegt also die „besondere Gefährdung"?

Artikel 9 BtxStV treibt den Datenschutz so weit, daß bundeseinheitliche Normen, wie zum Beispiel Abgabenordnung (AO) und Handelsgesetzbuch (HGB) nicht mehr ordnungsgemäß erfüllt werden können, weil durch die geforderte Anonymisierung beziehungsweise Löschung Nachweise nicht erbracht werden können — bis hin zur Umsatzsteuer, der man im einzelnen nicht die Seitenvergütung nachweisen kann, so daß das Telespiel der Kinder, das Kochrezept der Mutter etc. etc. in der geschäftlichen Nutzung des Vaters untergeht. Es erscheint absurd, daß über Datenschutzbestimmungen von Ländern die Ordnungsmäßigkeit des Rechnungswesens beeinträchtigt wird. (Das kommt davon, wenn sich Medienpolitiker unter dem Mäntelchen der „Kulturhüter" in Technik und Recht einmischen und sich nicht einmal raten lassen).

## Sicherungsmöglichkeiten

Btx-Anbieter und -Betreiber sind natürlich bemüht, ihre Systeme in allen Phasen der Datenverarbeitung so sicher wie möglich zu machen — schon im eigenen Interesse! Mit „Betreiber" definiert der BtxStV alle, die für Dritte Btx-Dienstleistungen erbringen: also die Deutsche Bundespost, Dienstleistungsrechenzentren und Btx-Agenturen. Diese Definition entspricht in etwa dem 4. Abschnitt BDSG.

Anbieter und Betreiber haben eine Reihe von Sicherungsmöglichkeiten, die teilweise das Btx-System bietet, teilweise nur im Rechnerverbund zu verwirklichen sind und teilweise erst noch endgültig freigegeben werden müssen, wie zum Beispiel die Chipkarte und „Aida".

Die nebenstehende Tabelle zeigt die Hierarchie der Sicherungsmöglichkeiten vom „closed shop" bis zur Verschlüsselung.

Die noch nicht so gebräuchlichen Begriffe dieser Übersicht sollen näher erläutert werden:

Zu 11: Zu Beginn der Btx-Sitzung wird die Uhrzeit = Ende der letzten Nutzung gezeigt. Stimmt sie nicht mit den eigenen Aufzeichnungen überein (Dokumentation ist bei Btx genauso wichtig wie in der EDV!), so sollte man sofort das Persönliche Kennwort — PK — ändern, um weiteren Mißbrauch zu verhindern.

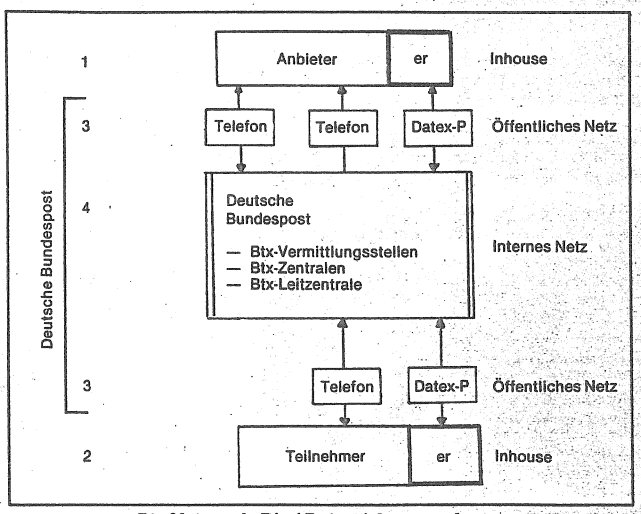
Zu 12: Das Abschalten nach Fehlversuchen erfordert neues Anwählen, das Zeit und Geld kostet und somit die Hemmschwelle für unrechtmäßige Nutzung höher setzt.

Zu 13: Die Transaktionsnummern — TAN — bewähren sich heute schon im Btx-Bankverkehr, der bereits über 10 000 Konten umfaßt. Die TAN ist gleichsam eine elektronische Einmalunterschrift. Sie wird vom Bankcomputer mittels Zufallsgenerator errechnet, und der Kunde erhält eine Liste mit 50 TANs in verschlossenem Umschlag am Bankschalter gegen Quittung (so ähnlich wie die Geheimnummer für den Bargeldautomaten). Die Zahlen kennt sonst nur noch der Bankcomputer. Bei jeder Transaktion = Überweisung, Verfügung etc. muß eine TAN in bestimmter Reihenfolge eingegeben werden und jede Nummer gilt nur für eine Transaktion. Je mehr Stellen die TAN hat, desto sicherer ist sie; Vier bis sechs Stellen sind üblich. Natürlich muß die TAN-Liste so sicher wie irgend möglich aufbewahrt werden. Andererseits kann ein Dieb mit der Liste allein nichts anfangen, da vorher immer noch ein Persönliches Kennwort eigegeben werden muß, das man nur im Kopf haben sollte. Wird eine Telefonleitung abgehört, erfährt der Abhörer sowohl PK als auch TAN. Wird länger abgehört, was allerdings sehr aufwendig ist, könnte man aus mehreren TANs den Algorithmus errechnen und damit die weiteren LANs ausrechnen. Um diese „Nutzung" unmöglich zu machen, gibt es das zweistufige TAN-Verfahren, bei dem nach Errechnung der Zahlen diese „geschüttelt", in eine willkürliche unsystematische Reihenfolge gebracht und dann erst ausgedruckt werden.

**Btx-Sicherheitssystem Organisatorische und technische Sicherheitsmöglichkeiten**

| | | |
|---|---|---|
| 01 | Geschütztes System — „Closed Shop" — | O/T |
| 02 | Datennetzsicherung | T |
| 03 | Systemkennwort | O/T |
| 04 | Modem-/Monitor-/Terminalkennung | T |
| 05 | Teilnehmer-Nummer (Abfragen/Dialog) | O |
| 06 | Persönliches Kennwort (Teilnehmer) | O/T |
| 07 | Anbieter-Nummer (Eingeben/Dialog) | O |
| 08 | Eingabe-Kennwort (Anbieter) | O/T |
| 09 | Mitglieder-/Konto-ö. Ä. Nummer | O |
| 10 | Sicherheitsgrenzen (Zugriffszeit/Betraghöhe u. Ä.) | O/T |
| 11 | Kontrolldaten (Uhrzeit letzter Nutzung) | T |
| 12 | Sicherheitsreaktionen (Abschalten nach 3 Fehlversuchen/Protokoll) | T |
| 13 | TAN (zweistufiger Zufallsgenerator) | T |
| 14 | Oberkellner-Methode (Datum + Uhrzeit ergänzen) | T |
| 15 | PIN PIN-Card/Chip-Card | T |
| 16 | Session-PIN „AIDA" | T |
| 17 | Verschlüsselung „End-to-End" | T |
| 18 | Den Menschen „einschalten" — Revision | O |

O = überwiegend organisatorische,
T = überwiegend technische Sicherheitsmöglichkeiten
O/T = beide Bereiche ergänzen sich




**Btx-Netzwerk: Die 4 Datensicherungsebenen**

## „Oberkellner-Methode"

So sicher die TANs auch sind, das Verfahren ist aufwendig und wegen der ausgedruckten Listen letztlich doch anfällig.

Zu 14: Die „Oberkellner-Methode" (die ehrenwerten Gastronomie-Mitarbeiter mögen verzeihen) benutzt Datum und gegebenenfalls auch noch Uhrzeit, die addiert, subtrahiert, multipliziert oder dividiert die zu übertragenden Daten verändern. Da jedes Datum und jede Uhrzeit einmalig sind, ist hier eine weitere Möglichkeit der Sicherung gegeben, die besonders in Verbindung mit anderweitiger Verschlüsselung große Sicherheit schafft.

Zu 15: Die Persönliche Identitätsnummer — PIN — ist die Weiterentwicklung des Persönlichen Kennworts — PK. Hierbei bedient man sich schon der Verschlüsselung, so daß die echte Nummer gar nicht mehr in Erscheinung tritt und somit von einem Gesetzesbrecher nicht benutzt werden kann. Die PIN ist vor allem bei Online-Verfahren interessant und besonders dann, wenn sie in einer PIN- oder Chip-Card gespeichert wird. Das ist eine Ausweiskarte im Scheckkartenformat, die auch wieder nur gemeinsam mit einem PK benutzt werden kann, um unerwünschte Nutzung bei Verlust zu vermeiden. Bei Online-Anwendungen besteht darüber hinaus noch die Möglichkeit, die Verschlüsselung bei jeder Transaktion zu ändern, wodurch auch Abhören uninteressanter wird.

## Individuelle Offline-Verschlüsselung

„Aida" ist eine Kombination und Verbesserung von TAN und PIN. Die Nachteile von TAN (Listenausdruck) und PIN (üblicherweise statistische Nummer) werden durch „Aida" nicht nur beseitigt, sondern weitere Vorteile hinzugefügt (Entwicklung Raymund Eisele, BIK, vergleiche CW

Fortsetzung von Seite 21

# Sechs richtige wahrscheinlicher als . . .

unrechtmäßigen Zugriff auf Datenbanksegmente, bieten gleichsam „elektronische Unterschrift". Die Datenströme selbst sind jedoch nur durch eine End-to-end-Verschlüsselung — also vom Teilnehmer bis in die Datenbank hinein und zurück — gegen Fälschung, Verfälschung oder Mißbrauch zu sichern.

Die Kryptologie bietet zwar viele Möglichkeiten und Geräte, nur ist der Aufwand dafür leider nicht gering und für einen Massendienst zu teuer. Daher werden heute nur besonders sensible geschlossene Benutzergruppen (GBG) damit ausgerüstet. Eine Erweiterung des „Aida"-Verfahrens, das weiter unten erläutert wird (siehe auch CW Nr. 23 vom 1. Juni 84, Seite 22) wäre hier eine sehr gute Hilfe für die DFU kleinerer Datenmengen.

## Fernmelderecht und Btx-Technik

In Bild 1 sind die Einrichtungen der Deutschen Bundespost aufgezeichnet, die zur Btx-Versorgung nötig sind. Sie unterliegen alle der Fernmeldehoheit mit dem Fernmelderecht, hier insbesondere der Fernmeldeordnung (FO), sowie dem Strafrecht. Basis hierfür ist Artikel 10 des Grundgesetzes — Brief-, Post- und Fernmeldegeheimnis. Als Ausnahme für die Überwachung gibt es das Grundgesetz 10 und Paragraph 100a StPO bei Verdacht auf schwere Straftaten, wofür jedoch gemäß Paragraph 100b StPO nur ein Richter zur Anordnung der Überwachung zuständig ist.

Die Fernmeldeordnung wurde durch die 22. Änderungsverordnung (ÄndVFO) ergänzt. Für den Datenschutz wurde dabei ein Absatz in den Paragraphen 38b FO eingefügt, der jedoch rein deklaratorische Bedeutung hat, da der Datenschutz hier sowieso Teil des Fernmeldegeheimnisses ist. Rein technisch nötige Daten werden am Ende einer jeden Btx-Nutzung sofort automatisch gelöscht. Bei Btx-Seiten, für die eine Vergütung verlangt wird, werden Teilnehmer- und Anbieternummer, Datum und Uhrzeit (Anfang und Ende) sowie Summe der Vergütung gespeichert, nicht die einzelnen abgerufenen Seiten. Zur Abrechnung mit Teilnehmern und Anbietern werden nur die Vergütungssummen in der Fernmelderechnung ausgedruckt; somit sind die Daten voll anonymisiert. Nur für Revisionsfälle (zum Beispiel das Einklagen von Forderungen) werden die gespeicherten Daten drei Monate im „Ulmer Datensumpf" aufbewahrt und dann automatisch gelöscht.

Somit ist rechtlich und technisch alles getan, um Datenschutz und Datensicherung nach den Regeln des BDSG sicherzustellen.

## Jeder ist „speichernde Stelle"

Unter den Btx-Teilnehmern (Oberbegriff) spielen die Anbieter von Btx-Informationen datenschutzrechtlich eine besondere Rolle. Für sie gelten natürlich erst einmal die Normen des BDSG, darüber hinaus aber auch Artikel 9 BtxStV ff. und damit eine gravierende Erweiterung des Begriffs der „Datei": Das ganze Btx-Angebot wird in Artikel 9 Absatz 5 als Datei definiert! Ob sich die Väter des BtxStV über die Konsequenzen im klaren waren? Jeder Bürger, der am Btx-Mitteilungsdienst teilnimmt, zum Beispiel eine Btx-Seite mit einer Gratulation zum Geburtstag absendet, wird mit zur „speichernden Stelle" (gemäß Paragraph 2 Absatz 3 Ziffer 1 BDSG)!

Die bereichsspezifische Datenschutzregelung des Artikel 9 geht — wie schon erwähnt — von einem „besonderen Gefährdungspotential" aus.

Dies ist unverständlich, da bei einem Btx-Kontakt, soweit der Teilnehmer nur „liest", der Anbieter überhaupt nichts davon erfährt, und — soweit der Teilnehmer zum Beispiel etwas bestellt oder sonstwie eine Willenserklärung von sich gibt — nur die Daten an den Absender geschickt werden, die der Teilnehmer (durch freiwilliges Drücken der Tasten 1 und 9) selbst freigibt. Dabei werden üblicherweise nicht mehr Fakten erhoben als bei einer telefonischen Bestellung oder einer Bestellpostkarte. Wo liegt also die „besondere Gefährdung"?

Artikel 9 BtxStV treibt den Datenschutz so weit, daß bundeseinheitliche Normen, wie zum Beispiel Abgabenordnung (AO) und Handelsgesetzbuch (HGB) nicht mehr ordnungsgemäß erfüllt werden können, weil durch die geforderte Anonymisierung beziehungsweise Löschung Nachweise nicht erbracht werden können — bis hin zur Umsatzsteuer, der man im einzelnen nicht die Seitenvergütung nachweisen kann, so daß das Telespiel der Kinder, das Kochrezept der Mutter etc. etc. in der geschäftlichen Nutzung des Vaters untergeht. Es erscheint absurd, daß über Datenschutzbestimmungen von Ländern die Ordnungsmäßigkeit des Rechnungswesens beeinträchtigt wird. (Das kommt davon, wenn sich Medienpolitiker unter dem Mäntelchen der „Kulturhüter" in Technik und Recht einmischen und sich nicht einmal raten lassen).

## Sicherungsmöglichkeiten

Btx-Anbieter und -Betreiber sind natürlich bemüht, ihre Systeme in allen Phasen der Datenverarbeitung so sicher wie möglich zu machen — schon im eigenen Interesse! Mit „Betreiber" definiert der BtxStV alle, die für Dritte Btx-Dienstleistungen erbringen: also die Deutsche Bundespost, Dienstleistungsrechenzentren und Btx-Agenturen. Diese Definition entspricht in etwa dem 4. Abschnitt BDSG.

Anbieter und Betreiber haben eine Reihe von Sicherungsmöglichkeiten, die teilweise das Btx-System bietet, teilweise nur im Rechnerverbund zu verwirklichen sind und teilweise erst noch endgültig freigegeben werden müssen, wie zum Beispiel die Chipkarte und „Aida".

Die nebenstehende Tabelle zeigt die Hierarchie der Sicherungsmöglichkeiten vom „closed shop" bis zur Verschlüsselung.

Die noch nicht so gebräuchlichen Begriffe dieser Übersicht sollen näher erläutert werden:

Zu 11: Zu Beginn der Btx-Sitzung wird die Uhrzeit = Ende der letzten Nutzung gezeigt. Stimmt sie nicht mit den eigenen Aufzeichnungen überein (Dokumentation ist bei Btx genauso wichtig wie in der EDV!), so sollte man sofort das Persönliche Kennwort — PK — ändern, um weiteren Mißbrauch zu verhindern.

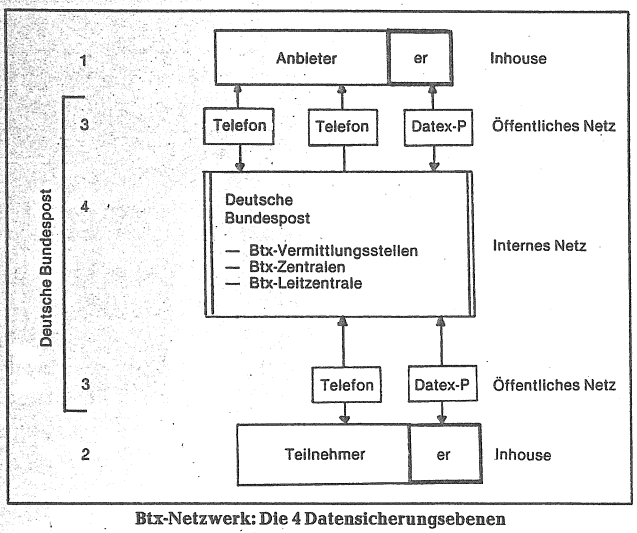
Zu 12: Das Abschalten nach Fehlversuchen erfordert neues Anwählen, das Zeit und Geld kostet und somit die Hemmschwelle für unrechtmäßige Nutzung höher setzt.

Zu 13: Die Transaktionsnummern — TAN — bewähren sich heute schon im Btx-Bankverkehr, der bereits über 10 000 Konten umfaßt. Die TAN ist gleichsam eine elektronische Einmalunterschrift. Sie wird vom Bankcomputer mittels Zufallsgenerator errechnet, und der Kunde erhält eine Liste mit 50 TANs in verschlossenem Umschlag am Bankschalter gegen Quittung (so ähnlich ausrechnen. Um diese „Nutzung" unmöglich zu machen, gibt es das zweistufige TAN-Verfahren, bei dem nach Errechnung der Zahlen diese „geschüttelt", in eine willkürliche unsystematische Reihenfolge gebracht und dann erst ausgedruckt werden.

**Btx-Sicherheitssystem Organisatorische und technische Sicherheitsmöglichkeiten**

| | | |
|---|---|---|
| 01 | Geschütztes System — „Closed Shop" — | O/T |
| 02 | Datennetzsicherung | T |
| 03 | Systemkennwort | O/T |
| 04 | Modem-/Monitor-/Terminalkennung | T |
| 05 | Teilnehmer-Nummer (Abfragen/Dialog) | O |
| 06 | Persönliches Kennwort (Teilnehmer) | O/T |
| 07 | Anbieter-Nummer (Eingeben/Dialog) | O |
| 08 | Eingabe-Kennwort (Anbieter) | O/T |
| 09 | Mitglieder-/Konto-ö. Ä. Nummer | O |
| 10 | Sicherheitsgrenzen (Zugriffszeit/ Betraghöhe u. Ä.) | O/T |
| 11 | Kontrolldaten (Uhrzeit letzter Nutzung) | T |
| 12 | Sicherheitsreaktionen (Abschalten nach 3 Fehlversuchen/Protokoll) | T |
| 13 | TAN (zweistufiger Zufallsgenerator) | T |
| 14 | Oberkellner-Methode (Datum + Uhrzeit ergänzen) | T |
| 15 | PIN PIN-Card/Chip-Card | T |
| 16 | Session-PIN „AIDA" | T |
| 17 | Verschlüsselung „End-to-End" | T |
| 18 | Den Menschen „einschalten" — Revision | O |

O = überwiegend organisatorische,
T = überwiegend technische Sicherheitsmöglichkeiten
O/T = beide Bereiche ergänzen sich




**Btx-Netzwerk: Die 4 Datensicherungsebenen**

## „Oberkellner-Methode"

So sicher die TANs auch sind, das Verfahren ist aufwendig und wegen der ausgedruckten Listen letztlich doch anfällig.

Zu 14: Die „Oberkellner-Methode" (die ehrenwerten Gastronomie-Mitarbeiter mögen verzeihen) benutzt Datum und gegebenenfalls auch noch Uhrzeit, die addiert, subtrahiert, multipliziert oder dividiert die zu übertragenden Daten verändern. Da jedes Datum und jede Uhrzeit einmalig sind, ist hier eine weitere Möglichkeit der Sicherung gegeben, die besonders in Verbindung mit anderweitiger Verschlüsselung große Sicherheit schafft.

Zu 15: Die Persönliche Identitätsnummer — PIN — ist die Weiterentwicklung des Persönlichen Kennworts — PK. Hierbei bedient man sich schon der Verschlüsselung, so daß die echte Nummer gar nicht mehr in Erscheinung tritt und somit von einem Gesetzesbrecher nicht benutzt werden kann. Die PIN ist vor allem bei Online-Verfahren interessant und besonders dann, wenn sie in einer PIN- oder Chip-Card gespeichert wird. Das ist eine Ausweiskarte im Scheckkartenformat, die auch wieder nur gemeinsam mit einem PK benutzt werden kann, um unerwünschte Nutzung bei Verlust zu vermeiden. Bei Online-Anwendungen besteht darüber hinaus noch die Möglichkeit, die Verschlüsselung bei jeder Transaktion zu ändern, wodurch auch Abhören uninteressanter wird.

## Individuelle Offline-Verschlüsselung

„Aida" ist eine Kombination und Verbesserung von TAN und PIN. Die Nachteile von TAN (Listenausdruck) und PIN (üblicherweise statistische Nummer) werden durch „Aida" nicht nur beseitigt, sondern weitere Vorteile hinzugefügt (Entwicklung Raymund Eisele, BIK, vergleiche CW



vom 1. Juni 84,
Apparate zur
Autorisierung —
merseite ein Tasc
sätzlichem Chip
und auf der Anb
Rechner) ein Zu
Beispiel IBM /1).
Eine Fortentwi
fahrens sollte
nicht nur Autor
tronische Unters
chen, sondern au
mengen zu vers
viele neue Einsa
sen und damit d
durch noch gr
noch preiswerte
können.
Über die Diskus
schutz darf nicht
daß für die Unter
tionen der Gehei
wichtiger ist, wei
stanz geht und ni
Daten von Mitarb
Lieferanten. We
mensdaten richt
geschützt werde
Bemühungen fü
Datensicherung
fast von allein. D
EDV gilt genau s
Eine besondere
Überlegungen b
nen Benutzergr
hier üblicherwe
bund gearbeitet
das Sicherheitss
da es beim Anl
ihm angewies
(zum Beispiel A
tern) liegt, die
keiten optimal zu

## Jede Wot

Hier liegt — n
größte Gefährd
Masse der — pr
noch viel zuw
wußtsein entwi
bei Teilnehmer
Verwaltung m
werden. Leider
tenschutz imm
Zwang an und
im Eigeninteres
richtig einschät
an die gedank
von EDV-Kennw
tionalen Widers
protokollierung,
mit dem Recht
verhindert werd
Doch zurück
letztlich jeden v
Fernseher im
heute Bestandt
werden. Jeder
letztlich zum An
er den Mitteil
Nachrichten abs
ren. Und damit k
tenverarbeitung
letzt ist ein Arg
„EDV für alle" —
tische Entwickl
Fortschritt der
würdigkeit der
puter, so wird s
des Büro, sond
nung „Rechenze
Ohne Blasphemi
der Bibel das BD
Haus — und w
auch noch der B
Ob diese Norr
„für den Hausge
Bildschirmtex
Datenschutz u
eine Sonderstel
nur, weil es ein
dafür gibt, sond
sofort die Pro
EDV bis hin zu
unendlich grof

Computerwoche 10. August 1984



vom 1. Juni 84, Seite 22). „Aida" = Apparate zur Identifikation und Autorisierung — ist auf der Teilnehmerseite ein Taschenrechner mit zusätzlichem Chip und Spezialtasten und auf der Anbieterseite (Externer Rechner) ein Zusatz zur CPU (zum Beispiel IBM /1).

Eine Fortentwicklung dieses Verfahrens sollte auch ermöglichen, nicht nur Autorisierung und „Elektronische Unterschrift" sicherzumachen, sondern auch kleinere Datenmengen zu verschlüsseln, wodurch viele neue Einsatzgebiete erschlossen und damit die Taschenrechner durch noch größere Stückzahlen noch preiswerter gemacht werden können.

Über die Diskussion um den Datenschutz darf nicht vergessen werden, daß für die Unternehmen und Institutionen der Geheimnisschutz oft noch wichtiger ist, weil es hier um die Substanz geht und nicht nur um ein paar Daten von Mitarbeitern, Kunden und Lieferanten. Wenn die Unternehmensdaten richtig verarbeitet und geschützt werden, ergeben sich alle Bemühungen für Datenschutz und Datensicherung im Sinne des BDSG fast von allein. Diese Erkenntnis der EDV gilt genau so für Btx!

Eine besondere Rolle spielen diese Überlegungen bei den Geschlossenen Benutzergruppen — GBG. Da hier üblicherweise im Rechnerverbund gearbeitet wird, gestaltet sich das Sicherheitssystem relativ leicht, da es beim Anbieter und dem von ihm angewiesenen Teilnehmern (zum Beispiel Außendienstmitarbeitern) liegt, die Sicherungsmöglichkeiten optimal zu nutzen.

## Jede Wohnung ein RZ

Hier liegt — neben dem Netz — das größte Gefährdungspotential, da die Masse der — privaten — Teilnehmer noch viel zuwenig Datenschutzbewußtsein entwickelt hat. Aber auch bei Teilnehmern aus Wirtschaft und Verwaltung muß noch viel getan werden. Leider sehen viele den Datenschutz immer noch als lästigen Zwang an und können die Vorteile im Eigeninteresse immer noch nicht richtig einschätzen! Man denke nur an die gedankenlose Bestimmung von EDV-Kennworten oder den emotionalen Widerstand gegen Zugangsprotokollierung, die dann auch noch mit dem Rechtsschein des BetrVG verhindert werden sollen.

Doch zurück zur Privatsphäre, die letztlich jeden von uns angeht: Jeder Fernseher im Wohnzimmer kann heute Bestandteil einer DV-Anlage werden. Jeder Teilnehmer kann letztlich zum Anbieter werden, wenn er den Mitteilungsdienst benutzt: Nachrichten absenden, kommunizieren. Und damit kann jeder Bürger Datenverarbeitung betreiben. Nicht zuletzt ist ein Argument für Btx auch „EDV für alle" — eine sehr demokratische Entwicklung! Nimmt man den Fortschritt der EDV hinzu, die Preiswürdigkeit der Mikro- und Heimcomputer, so wird sehr bald nicht nur jedes Büro, sondern auch jede Wohnung „Rechenzentrum" sein können. Ohne Blasphemie gehört dann neben der Bibel das BDSG in jedes deutsche Haus — und wenn der Teufel will, auch noch der Btx-Staatsvertrag . . .

Ob diese Normen aber das richtige „für den Hausgebrauch" sind?

Bildschirmtext nimmt hinsichtlich Datenschutz und Datensicherung eine Sonderstellung ein. Aber nicht nur, weil es einen Btx-Staatsvertrag dafür gibt, sondern weil durch Btx ab sofort die Problematik dezentraler EDV bis hin zur Mikrovernetzung in unendlich großem Umfang auftritt und Btx im Rahmen der Bürokommunikation Möglichkeiten eröffnet, die nun allmählich technisch und wirtschaftlich das „Büro der Zukunft" näherrücken lassen.

Das Datenschutzbewußtsein ist noch sehr unterentwickelt. Das gilt genauso für das Datensicherungsbewußtsein. Wer bringt den Leuten bei, daß sie letztlich alles nur aus Eigenliebe tun, daß Datenschutz auch Schutz der eigenen Daten und Datensicherung auch Schutz der eigenen Firma bedeutet? Hier nützen Gesetze und Verordnungen sehr wenig! Natürlich müssen sie stets der Entwicklung von Technik, Gesellschaftspolitik und Rechtsnormen angepaßt werden, wobei dies immer bedeuten kann: im Rahmen der EG, der UNO.

Auf keinen Fall im Rahmen der „Kultur" kleiner Regionen, die als Bundesländer ihre Einwohner bevormunden und andererseits vom „mündigen Bürger" schwärmen. Wie soll man sich mit seinem Nachbarn gut verstehen, wenn schon jedes Bundesland für die „Neuen Medien" ein anderes Gesetz entwickelt.

Was wir wirklich brauchen, sind ständig bessere Sicherungsmöglichkeiten für Hard- und Software — gerade auch in der Größenordnung der Mikros und Btx-Terminals. Das sind Erkenntnisse, die schon seit vielen Jahren formuliert worden sind.

Bei jeder neuen Technik können auch neue Gefahrenpotentiale entstehen, zum Beispiel die Möglichkeit zur Erstellung von „Persönlichkeitsprofilen". Hier ist klare Definition und Sensibilisierung aller nötig, um einerseits Mißbrauchsrisiken und deren mögliche Folgen herauszuarbeiten und andererseits aber auch unberechtigtes Mißtrauen abzubauen, damit endlich unvoreingenommenes Problembewußtsein geschaffen wird.

Das sagt uns zum Beispiel, daß Btx keine „besondere Gefahr" darstellt, daß aber andererseits der Schutz auch „nur" so gut ist wie bei der allgemeinen Verarbeitung personenbezogener Daten.

Basis für alle Bemühungen ist auch hier der Mensch, der sensibler reagieren — und vor allem agieren — muß als bisher; denn sehr bald ist jeder Bürger nicht nur „Betroffener", sondern auch — nach dem Willen des BtxStV — „Speichernde Stelle". Und somit haben die „Haushaltungsvorstände" ab sofort eine neue Funktion: Sie verpflichten in einer „elektronischen Weihestunde" ihre Lieben auf Paragraph 5 des BDSG . . .