Kein Zugang für Unbefugte

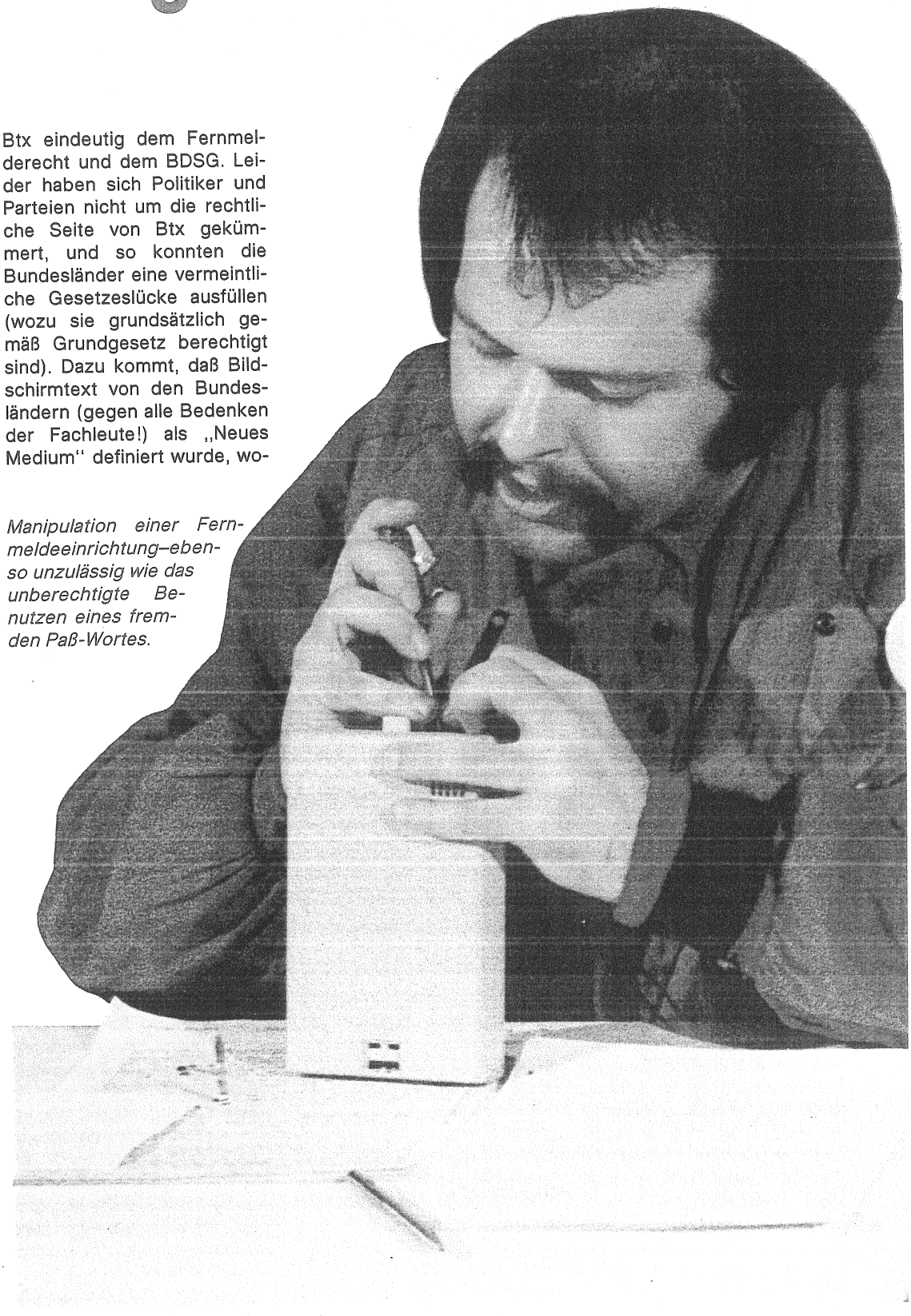
Wie Btx-Daten geschützt und gesichert werden

Ein Hacker bei der Manipulation am Modem: Millionen Zuschauer sahen es im „heute journal". Datenschutz und Datensicherheit rückten verstärkt ins Bewußtsein der Öffentlichkeit wie der Insider. Doch um die Rechtssicherheit bei Btx ist es schlecht bestellt. Beiträge verschiedener Fachleute bringen im Folgenden Licht ins Durcheinander von Recht und Risiko, von Fehlern und Chancen.

Dem Thema „Datensicherheit und Datenschutz bei Btx" wird man nur gerecht, wenn man juristische, organisatorische und technische Gesichtspunkte gleichermaßen berücksichtigt. Da gibt es eine Vielzahl ernstzunehmender Fakten, die oft viel zu emotional und ohne hinreichenden Sachverstand diskutiert werden. Dies ist die Meinung von Diplom-Kaufmann Wolfgang Gorn, Sachverständiger für Informatik, Unternehmensberater und Externer Datenschutzbeauftragter. Seiner Darstellung der Problematik hat er ein Zitat vorangestellt: „Des Hackers Freud ist des Datenschützers Leid" (Homo electronicus).

Wenn man ausrechnen kann, daß ein unberechtigtes Eindringen in das Btx-System eine geringere Wahrscheinlichkeit hat als 6 Richtige im Lotto, so ist das schon ziemlich beruhigend. Wenn man darüber hinaus bedenkt, daß das Bundesdatenschutzgesetz (BDSG) schon seit Jahren nicht gerade unbedeutenden Schutz bietet, wenngleich es auch in einigen Punkten verbesserungswürdig ist, so ist doch schon einiges getan. Die größte Schwachstelle ist z. Zt. das „offene Netz". Das, was die größten Vorteile bietet, birgt auch die größten Gefahren! Wichtig ist, daß man alle Möglichkeiten, die es heute und morgen organisatorisch und technisch gibt, auch intensiv nutzt – und da ist in der Praxis noch sehr viel zu tun – bis hin zu zügiger internationaler Normung.

Btx ist technisch gesehen Fernmeldedienst und EDV-Peripherie. Damit unterliegt Btx eindeutig dem Fernmelderecht und dem BDSG. Leider haben sich Politiker und Parteien nicht 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, wo-



Manipulation einer Fernmeldeeinrichtung–ebenso unzulässig wie das unberechtigte Benutzen eines fremden Paß-Wortes.

für – entsprechend der Kulturhoheit der Länder, aber auch hier schon unsinnig – Landesrecht zuständig ist.

Auf diese Weise haben wir heute neben dem Fernmelderecht – hier insbesondere die Fernmeldeordnung – FO – und dem BDSG auch noch den Staatsvertrag der Bundesländer zu Btx – BtxStV – zu beachten. Er 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, wie etwa der G.U.I.D.E.-Arbeitskreis Datenschutz und Datensicherung sowie Gremien der AWV oder des DIHT. Dies gilt besonders für die Bestimmungen des Art. 9 zum Datenschutz, aber auch z.B. für die unklaren Formulierungen des Art. 8 zur Werbung, der mehr Unsicherheit schafft, als er klärend wirkt.

Btx wird im Staatsvertrag einerseits technisch eingeengt (Ausschluß der Bewegtbildübertragung, die mit breitbandigen Netzen kommt und für Btx viele Vorteile bringen wird) und andererseits juristisch so einseitig als „Medium" mit allen Konsequenzen definiert, daß die Kulturhoheit der Länder unabdingbar erscheint.

Was sind das für Länder, die im Zeitalter der UNO und EG eine solche Hoheit reklamieren, die mehr als „Steinzeit" bedeutet? Hier wird versucht, Bundes- und internationales Recht in einer Weise zu reglementieren, die diesen Staatsvertrag als rechtspolitisch und rechtssystematisch 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 z.B. Datenschutz zum Prügelknaben falsch verstandenen Verbraucherschutzes. Österreich ist ein trauriges Beispiel für diese Perversion (Verbot von Geschäftsabschlüssen und Bankaktivitäten), wo gerade österreichische Wissenschaftler, Techniker und Kaufleute mit dem „mupid" viel für Btx getan haben.

Wolfgang Gorn

Die amtliche Begründung zu Art. 9 BtxStV – Datenschutz – geht von einem „besonderen Gefährdungspotential von Btx" aus. Es wird hier völlig verkannt, daß Btx nur eine technische Variante moderner Datenfernübertragung – DFÜ – im Rahmen der Datenverarbeitung – DV – ist. Und hierfür gilt nun einmal das BDSG. Wenn also irgendein Regelungsdefizit vorliegt, das erst einmal sorgfältig analysiert und definiert werden muß, dann muß dies im Rahmen einer BDSG-Novellierung geklärt werden und vor allem nicht von Politikern auf Landesniveau, die von der Materie keine Ahnung haben.

Gefahr Nr. 1: das öffentliche Netz

Bei allen Vorteilen des öffentlichen Netzes (Verfügbarkeit, Ausdehnung, Kosten) müssen wir klar sehen, daß einerseits hier die umfangreichste Gefahrenquelle liegt, andererseits Btx aber genauso sicher (unsicher) wie das Telefonieren ist: Hier liegt die eigentliche Gefahr der Datenverarbeitung und Datenübertragung.

Wenn auch die Kabel in Deutschland überwiegend unterirdisch liegen, so geben Endverteiler und die Verkabelung in Gebäuden genügend Möglichkeiten für kriminelle Aktivitäten mit einfachem technischem Aufwand.

„PIN" und „TAN" bieten Sicherheit gegen 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, denn das Anzapfen einer Telefonleitung und das Zwischenschalten eines PC kann z.B. „Online" simulieren und Schäden ermöglichen.

Die Kryptologie bietet heute 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 GBGs damit bestückt.

Eine Erweiterung des „AIDA"-Verfahrens und der Chipkarten-Technologie wären hier z.B. eine sehr gute Hilfe für die DFÜ.

Gefahr Nr. 2: Systemschwächen

Jedes EDV-System kann orgware-, hardware- und software-Schwächen haben.

Dies gilt um so mehr dann, wenn ein System (zu) schnell und von (zu) vielen Leuten entwickelt wird. Hier hat zweifellos die Deutsche Bundespost ohne zwingenden Grund zu sehr getrieben und die IBM trotz ihrer weltweiten Erfahrungen sich treiben lassen. Sie haben sich verhalten wie mittelmäßige Unternehmer, die nicht begreifen wollen, daß all das, was letztlich so elegant aussieht, viel und lange harte Arbeit erfordert.

Je besser (und damit zwangsläufig länger) die Vorbereitung, desto besser das Ergebnis: eine – besonders auch EDV-Binsenweisheit!

Während orgware und hardware einigermaßen „im Griff" sind, kann man das – natürlich – von der software nicht sagen, was jeder EDV-Kundige versteht.

Ein System dieser Dimension und Komplexität ist nur schwer überschaubar und braucht lange, um bis in die letzten Feinheiten – die aber sehr sicherheitsrelevant sein können! – ausgetestet zu werden.

Über den schönen bunten Bildchen vergessen viele diese Realität.

Das ist auch der Grund, warum uns intelligente Hacker „das Gruseln lehren" können.

Erkenntnis daraus: entweder warten, bis Btx weiter ausgetestet ist (und Verschlüsselung möglich wird) oder mit gewissen Risiken arbeiten, wobei festgestellt werden muß, daß uns gewiß noch nicht alle bekannt sind.

Für den, der heute schon mit Btx arbeiten will – wofür es übrigens viele gute Gründe gibt – ist es also um so wichtiger, alle möglichen Sicherheitsmaßnahmen – siehe Bild 2 – zu nutzen.

Übrigens: die vierte Systemschwäche muß immer besonders sorgfältig beobachtet werden: der „SYSOP", der System-Operator, der alles kann und darf und ohne den nichts läuft ... (durch „menschliches Versagen" sind schon Züge entgleist!).

Datenschutz und Datensicherung beim Anbieter

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 Art. 9 BtxStV ff. und damit eine gravierende Erweiterung des Begriffs der „Datei": das ganze Btx-Angebot wird in Art. 9 Abs. 5 als Datei definiert. Ob sich die Väter des BtxStV über die Konsequenzen im klaren waren?

Jeder Bürger, der am Btx-Mitteilungsdienst teilnimmt, z.B. eine Btx-Seite mit einer Gratulation zum Geburtstag absendet, wird damit zur „Speichernden Stelle" gem. § 2 Abs. 3 Ziff. 1 BDSG.

Die bereichsspezifische Datenschutzregelung des Art. 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. Erst wenn der Teilnehmer etwas bestellt oder sonstwie eine Willenser-

klärung von sich gibt – werden nur die Daten an den Absender geschickt, die der Teilnehmer (durch freiwilliges Drücken der Tasten 1+9!) selbst freigibt, wobei er durch den Hinweis „P" in Zeile 24 noch auf die Übermittlung personenbezogener Daten aufmerksam gemacht wird (Verbesserungsvorschlag: „P" gelb, blinkend, ggf. in Zeile 1). Dabei werden üblicherweise nicht mehr Fakten erhoben als bei einer telefonischen Bestellung oder einer Bestell-Postkarte. Wo liegt also die „besondere Gefährdung"?

Art. 9 BtxStV treibt den Datenschutz so weit, daß Bundesrecht wie z.B. Abgabenordnung – AO – und Handelsgesetzbuch – HGB – nicht mehr ordnungsgemäß erfüllt werden kann, weil durch die geforderte Anonymisierung bzw. Löschung erforderliche Nachweise nicht erbracht werden können – bis hin z.B. zur Umsatzsteuer, der man im einzelnen nicht die Seitenvergütung nachweisen kann. Es ist einfach absurd, daß über Datenschutzbestimmungen von Ländern z.B. auch die bundeseinheitliche Ordnungsmäßigkeit des Rechnungswesens beeinträchtigt wird: Das kommt davon, wenn sich „Kulturhüter" in Recht und Technik einmischen und sich nicht einmal raten lassen.

Möglichkeiten zur sicheren Organisation und Technik

Btx-Anbieter und -Betreiber sind natürlich bemüht, ihre Systeme in allen Phasen der Datenverarbeitung so sicher wie möglich zu machen – allein schon in eigenem Interesse.

Mit „Betreiber" definiert der BtxStV alle, die für Dritte Btx-Dienstleistungen erbringen: also die Deutsche Bundespost, Dienstleistungs-Rechenzentren 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 der DBP selbst bietet, teilweise nur im Rechnerverbund zu verwirklichen sind und teilweise erst noch endgültig freigegeben werden müssen, wie z.B. „AIDA" oder die Chipkarten.

Die Tabelle zeigt die Hierarchie der Sicherungsmöglichkeiten vom „closed shop" bis zur Verschlüsselung, wobei der Mensch – bei aller Technik auch hier – immer seine steuernde und kontrollierende Funktion behält: mit allen Vor- und Nachteilen.

Zu 02: Im offenen Netz liegt mit die größte Gefahr. Seine Sicherung ist daher grundlegend wichtig für alle Nutzungen der DFÜ.

Leitungs-Protokolle haben hierbei eine wichtige Funktion, da sie einerseits Störungen dokumentieren (Datensicherung), andererseits aber auch kriminelle Manipulationen festhalten können (Datenschutz/Geheimnisschutz), z.B. auch unberechtigte Zugriffsversuche.

Zu 04: Wenn sich ein Teilnehmer „freizügig" schaltet, um von beliebigen Terminals aus ins System einsteigen zu können, verliert er einen Sicherheitsfaktor, die Modem-Kennung. Es bleibt ihm nur sein persönliches Kennwort.

Gutes Sicherheitssystem braucht mindestens zwei Stufen

Da jedoch jedes gute Sicherheitssystem mindestens zwei Stufen braucht, sollte hier die Deutsche Bundespost mit ihren Verbesserungen ab Februar '85 auch eine „Ersatz-Kennung" bieten, was technisch kein Problem darstellt: Sobald sich ein Teilnehmer „freizügig" schaltet, sendet ihm Ulm eine Ersatz-Kennung (errechnet durch einen Zufalls-Generator), die solange gilt, bis die Freizügigkeit beendet wird. Wer nun die Freizügigkeit nicht generell schaltet, sondern nur stunden-, tageweise, der erhält eine gute, zusätzliche Sicherheit, da bei jeder „Freizügig"-Schaltung eine neue Ersatz-Kennung vergeben wird.

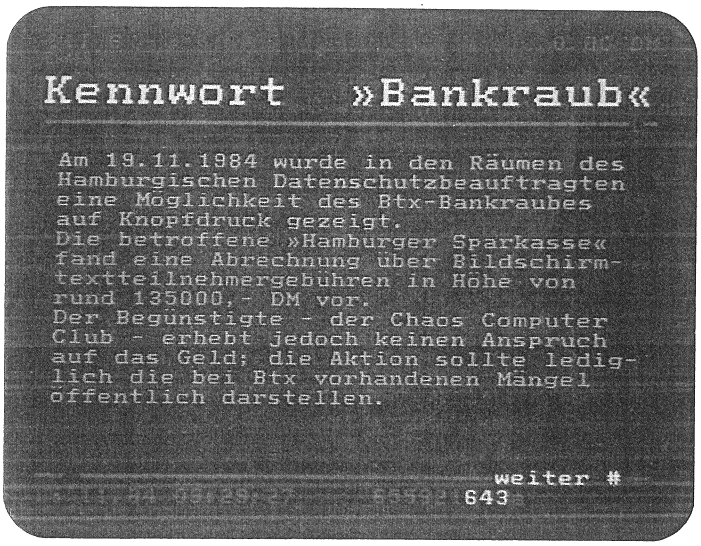
Zu 11: Zu Beginn jeder Btx-Sitzung wird die Uhrzeit = Ende der letzten Nutzung gezeigt. Stimmt sie nicht mit den eigenen Aufzeichnungen überein (Dokumentation ist bei Btx genauso wichtig wie in der EDV!), so sollte man sofort das persönliche Kennwort ändern, um weiteren Mißbrauch zu verhindern.

Zu 12: Das Abschalten nach Fehlversuchen erfordert neues Anwählen, das Zeit und Geld kostet und somit die Hemmschwelle für unrechtmäßige Nutzung höher setzt. Nach 3×3 Fehlversuchen wird automatisch endgültig abgeschaltet!

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 Einmal-Unterschrift. (Vergleiche „Btx Praxis" Heft 8/84, S. 13 ff.)

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

Zu 15: Die Persönliche Identitäts-Nummer (PIN) ist die Weiterentwicklung des passwords. Hierbei bedient man sich der Verschlüsselung, so daß die echte Nummer gar nicht mehr in Erscheinung tritt und somit von einem Gesetzesbrecher nicht benutzt werden kann.



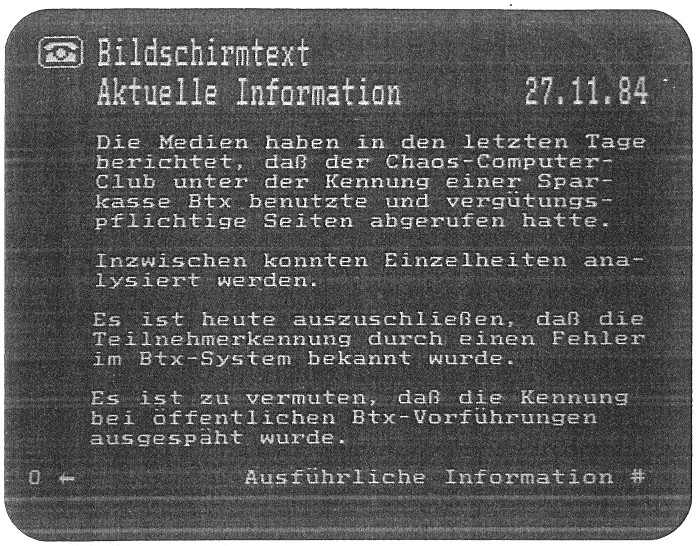
Großspurig sprachen die Hacker vom „Bankraub" in Hamburg, der aber keiner war . . .

Btx-Sicherheitssystem

Hierarchie der organisatorischen und technischen Möglichkeiten

01	Geschütztes System – „Closed Shop" –	O/T
02	Datennetz-Sicherung/ Leitungs-Protokolle	O/T
03	System-Organisation/ System-Kennwort	O/T
* 04	Modem-/Monitor-/Terminal-Kennung	O/T
* 05	Teilnehmer-Nummer (Abfragen/Dialog)	O
* 06	Persönliches Kennwort/Paßwort persönliche Identifizierungs-Nummer – PIN –	O/T
* 07	Anbieter-Nummer (Eingeben/Dialog)	O
* 08	Eingabe-Kennwort (Anbieter) Wird kommen – wie bei Prestel)	O/T
09	Mitglieder-/Konto- o. ä. Nummer	O
10	Sicherheitsgrenzen (Zugriffzeit/Betraghöhe u. ä.)	O/T
* 11	Kontrolldaten (Uhrzeit letzte Nutzung)	T
* 12	Sicherheitsreaktion (Abschalten nach 3 × 3 Fehlversuchen)	T
13	TAN (2stufiger Zufallsgenerator/ + Quittung)	O/T
14	Chronologische Sicherheit („Oberkellner-Methode)	T
15	PIN-Card / (Ein-)Chip-Card	T
16	Einmal-Verschlüsselung	T
17	Session-PIN/TAN-„AIDA"	T
18	Verschlüsselung End-To-End	T
19	Rückspiegeln (Echoplexing)	T
20	Den Menschen „Einschalten" = Revision	O/T

O = überwiegend organisatorische, T = überwiegend technische Sicherungsmöglichkeiten, O/T = beide Bereiche ergänzen sich, * = Sicherheits-Standard der Deutschen Bundespost).



. . . viel eher ermöglichte mangelnde Geheimhaltung des Paß-Wortes den Zugang.

Zu 16: Bei on-line-Anwendungen besteht darüber hinaus noch die Möglichkeit der Einmal-Verschlüsselung, d.h. die Verschlüsselung bei jeder Transaktion zu ändern, wodurch auch Abhören uninteressant wird.

Zu 17: „AIDA" Gleich dem Triumphmarsch von Verdi ist „AIDA" die Krönung von TAN und PIN. Die Nachteile von TAN (Listenausdruck) und PIN (üblicherweise statische Nummer) werden durch „AIDA" nicht nur beseitigt, sondern weitere Vorteile hinzugefügt (Entwicklung R. Eisele, BIK). „AIDA" = Apparate zur Identifikation und Autorisierung – ist auf der Teilnehmerseite ein Taschenrechner mit zusätzlichem Chip und Spezialtasten (geplanter Preis ca. 60 DM) und auf der Anbieterseite (Externer Rechner) ein Zusatz zur CPU (z. B. IBM/1). (Vgl. „Btx Praxis" Heft 7/84, S. 13). Wenn „AIDA" jedoch nicht bald auf den Markt kommt, wird sie von der Chipkarte überholt werden und ggf. nur noch für Spezialanwendungen interessant sein.

Zu 18: Die Verschlüsselung „end-to-end" ist letztlich die einzig sichere Methode – wenn man mit „Einmal-Verschlüsselung" arbeitet, d.h. wenn für jede Session ein anderer Schlüssel verwendet wird.

Zu 19: Das Echoplexing-Verfahren gibt in Verbindung mit der TAN-Quittung die Gewißheit, daß man erst die Transaktion als endgültig anerkennt („19"), die einem aus dem externen Rechner zurückgespiegelt worden ist.

Zur Zeit läuft im Frankfurter Raum ein Versuch mit Magnetkarten-Telefonen „Makatel", Telefonen also, die eine Magnetkarten-Leser-Station integriert haben. Auf diese Weise hoffen z.B. Kreditkartenorganisationen ihr Risiko in den Griff zu bekommen, indem bei jedem Kreditkartenkauf eine „Online"-Verbindung zur Zentrale geschaltet wird, um Berechtigung, Sperrung etc. zu prüfen. Leider hat man sich hier der unsicheren und nur wenige Möglichkeiten bietenden Magnetkartentechnik bedient, die noch nie viel getaugt hat (dafür aber billig ist).

Die Erkenntnis für Btx daraus: die Richtung ist nicht schlecht, nur die Technik überholt. Als „Chikatel" (Chipkartentelefon) würden auch für Btx sehr gute Möglichkeiten geboten.

Es ist zu hoffen, daß die Hersteller hier sehr bald entsprechende Geräte auf den Markt bringen, um die DFÜ allgemein sicherer zu machen.

Geheimnisschutz ist so wichtig wie Datenschutz

Über der 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 alle Unternehmensdaten richtig verarbeitet und geschützt werden, ergeben sich die Bemühungen für Datenschutz und Datensicherung im Sinne des BDSG fast von allein: Diese Erkenntnis der EDV gilt genauso für Btx als EDV-Peripherie!

Eine besondere Rolle spielen diese Überlegungen bei den geschlossenen Benutzergruppen – GBG –. Da hier üblicherweise im Rechnerverbund gearbeitet wird, gestaltet sich das Sicherheitssystem leichter, da es beim Anbieter und den von ihm abhängigen Teilnehmern (z.B. Außendienstmitarbeitern) liegt, die in Bild 3 aufgezeigten Sicherungsmöglichkeiten optimal zu nutzen.

Datenschutz und Datensicherung beim Teilnehmer

Hier liegt – neben offenem Netz und Systemschwächen – das 3. Gefährdungspotential, da die Masse der (privaten) Teilnehmer noch viel zu wenig 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 selbst im Eigeninteresse immer noch nicht richtig einschätzen. Man denke nur an die gedankenlose Bestimmung von EDV-Kennworten oder den emotionalen Widerstand gegen Zugangsprotokollierungen, 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. Und damit kann jeder Bürger Datenverarbeitung betreiben. Nicht zuletzt ist Btx auch „EDV für alle" – eine demokratische Entwicklung.

Nimmt man den Fortschritt der EDV hinzu, die Preiswürdigkeit der PC und Heimcomputer, so wird sehr bald nicht nur jedes Büro, sondern auch jede Wohnung „Rechenzentrums-Außenstelle" 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?

Telematik erschwert Datenschutz und Datensicherung

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

Dabei verschmelzen die Netze in einigen Jahren zum ISDN und alle Geräte werden multifunktional, wie es der „mupid" als Kombination von PC und Btx-Gerät schon seit Jahren zeigt.

Das Bewußtsein für den Datenschutz noch weiterentwickeln

Das Datenschutz-Bewußtsein ist – wie schon oben angedeutet – leider bei Privaten, Selbständigen und vielen kleinen (und auch größeren) Unternehmen noch sehr unterentwickelt.

Das gilt genauso für das Datensicherungs-Bewußtsein. 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

nur 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 ausländischen Nachbarn gut verstehen, wenn schon jedes Bundesland für die „Neuen Medien" ein anderes Gesetz entwickelt und damit Information und Kommunikation schlimmer reglementiert als die Inquisition?

Was wir wirklich brauchen sind ständig bessere Sicherheitsmöglichkeiten für hard- und software – gerade auch in der Größenordnung der PCs und Btx-Terminals. Das sind Erkenntnisse, die schon seit vielen Jahren formuliert worden sind.

Datenschutz darf nicht zum Täterschutz werden.

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 als „Herr der Daten" 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 § 5 BDSG . . .

Zum Thema „Datenschutz i.S. BDSG + BtxStV" muß eines ganz klar gesagt werden, was übrigens für die gesamte Rechtsproblematik gilt:

Datenschutz darf auch hier nicht zum Täterschutz pervertieren! Die Deutsche Bundespost muß im Interesse der Btx-Teilnehmer vielleicht sogar noch etwas mehr protokollieren und dokumentieren, als heute schon einigen beamteten Datenschützern recht ist!

Die Angst vor „1984" darf nicht so weit gehen, daß daraus Möglichkeiten für Rechtsverletzungen entstehen und Rechtsverfolgung unmöglich gemacht oder zumindest erschwert wird.

Juristisch „im Griff"

Die Bemühungen, den Hamburger Vorfall juristisch in Griff zu bekommen, gehen voran. „Welche Straftatbestände hätten die Hacker erfüllt, wenn sie auf ihrem Entgelt bestanden hätten?". Antwort eines Juristen: „Hier ist nach drei Straftatbeständen zu unterscheiden: Hätte die Hamburger Bank verwundert und zähneknirschend bezahlt, so hätte es sich um vollendeten Betrug gehandelt (Höchststrafe: Freiheitsstrafe von 5 Jahren, in besonders schweren Fällen bis zu 10 Jahren). Hätte sich die Bank geweigert zu zahlen, so läge versuchter Betrug vor. Die unentgeltliche Erschleichung von Fernmeldenetzleistungen durch die Hacker, um auf Gebührenkosten der Bank an ihr eigenes entgeltpflichtiges Angebot zu kommen, dürfte ‚Automatenmißbrauch' sein (Höchststrafe 1 Jahr). Die unberechtigte Benutzung eines fremden Paßwortes ist nach Art. 14 Staatsvertrag eine Ordnungswidrigkeit."

Anliegen und Mechanismen der Datensicherung

Kontrolle in zahlreichen Schritten

Ein Interesse an der Sicherung von Daten, die sich im Verkehr befinden und gespeichert werden können, haben sowohl die Benutzer des Btx-Dienstes wie der Betreiber Post und die einzelnen Anbieter. Hans Peter Lang von der Frankfurter IBM-Geschäftsstelle faßt die einzelnen Anliegen zusammen und stellt die Mechanismen zur Datensicherung dar. In den Tabellen analysiert er die gesetzlichen Regelungen und die Speichermöglichkeiten sowie mögliche Gefahren.

1. Die Datensicherungsanliegen beim Benutzer (Btx-Teilnehmer)

Die Datensicherungsanliegen des Benutzers können in Sicherungsanliegen aus Privatsphäreschutzbetrachtung und Sicherungsanliegen aus Vermögensschutz unterteilt werden.

a) Sicherung der Privatsphäreschutz-Anliegen am Endgerät des Benutzers:

- Abrufinformation für alle: Kein Anliegen.
  Btx-Seitenangebote sind der Öffentlichkeit frei verfügbare Angebote (neue Technik für alte Inhalte).
- Abrufinformation für Gruppen: Systemkontrolle.
  Abruferlaubnis darf nur erhalten, wer sich als Abrufberechtigter mit persönlicher Kennung ausweist (Identification/Verification).
  Nur dieser darf auf die kontrollierte Ressource zugreifen (Authorization).
- Empfänger als Mitglied einer Gruppe: Systemkontrolle.
  Die bereitgestellte Information darf nur mit der persönlichen Kennung des Benutzers (Identification/Verification) angenommen werden.
- Empfänger bei Individualkommunikation: Systemkontrolle.
  Die bereitgestellte Information darf nur mit der persönlichen Kennung des Benutzers (Identification/Verification) angenommen werden.
- Dialog mit externen Rechnern:
  Schritt 1: Vorphase eines Dialogs: Kein Anliegen.
  Der Benutzer „blättert" im allgemein verfügbaren Informationsangebot des Btx-Systems.
  Schritt 2: Eintritt in einen Dialog: Systemkontrolle.
  Der Benutzer fordert, daß er und somit alle anderen Mitbenutzer beim externen Rechner eindeutig identifiziert und berechtigt sind (Identification/Verification/Authorization).

b) Sicherung von Vermögensschutz-Anliegen am Endgerät des Benutzers:

- Alle angebotenen Anwendungsarten: Systemkontrolle.
  Benutzer fordert kontrollierte Zurechnung von Gebühren (Leitungskosten) und Entgelten (gebührenpflichtige Btx-Seiten). Dieses Anliegen, nicht der Privatsphäreaspekt, fordert selbst bei Abrufinformation für die Allgemeinheit die persönliche Kennung des

Medium	Daten über . . .	Speichernde Stelle	Hat der Teilnehmer Kenntnis?
Rundfunk, Fernsehen, Videotext	Person (Name, Adresse . . .)	Gebühreneinzugszentrale	Ja (Anmeldung)
Bildschirmtext	Person	Betreiber	Ja (Anmeldung)
	beanspruchte Dienste	Betreiber	Nein
	Einkommen und Vermögen	Anbieter	Ja (Dispositionen)
	Einkaufsverhalten	Anbieter	Ja (Einkäufe)
	Reiseverhalten	Anbieter	Ja (Buchungen)
Telefon/Bildtelefon	Person	Betreiber	Ja (Anmeldung)
Kabel-/Pay-TV	Person	Veranstalter?	Ja (Anmeldung)
	Sehgewohnheiten	Veranstalter?	Ja? (Buchung)
Offene Kanäle	Person?	Veranstalter	Ja (Anmeldung)
Rückkanäle	Person	Veranstalter?	Ja? (Anmeldung)
	Meinungen und dgl.	Veranstalter?	
Kabeltext	Person	Betreiber?	Ja (Anmeldung)
	beanspruchte Texte	Betreiber?	Nein
Fernwirkdienste	Person und ihr Verhalten	Veranstalter?/ Anbieter	Ja?

Übersicht über die mit den vorhandenen und künftigen Medien verbundene Datenspeicherung

Benutzers (Identification/ Verification).
- Mitbenutzung des Endgerätes.
  Das Btx-System soll dem Benutzer die Möglichkeit bieten, „Mitbenutzer" zu bestimmen, deren Identifikation er selbst ins System eingibt und verwaltet. Auch Mitbenutzer sollen nur mit persönlicher Kennung zum System zugreifen.
- Es liegt in der Verantwortung des Benutzers, zu bestimmen, ob andere Personen (z. B. Familienmitglieder) anwesend sein dürfen, wenn der systemberechtigte Benutzer mit dem Btx-System bestimmte Arbeiten durchführt.

2. Beim Betreiber (Btx-Steuerung)

Die Btx-Steuerung hat als „Service-Einrichtung" keine eigenen Btx-Informationen im System. Die Btx-Steuerung
- verwaltet die ihr von Einzelpersonen, Unternehmen, Behörden (auch DBP selbst) zur Verfügung gestellten Informationsangebote
- und ermöglicht die Kommunikation der Benutzer untereinander oder mit externen Rechnern.

Das Informationsmaterial in Btx besteht aus:
- den der Btx-Zentrale zur Verfügung gestellten Informationsseiten
- den Mitteilungen, die zwischengespeichert werden müssen, damit sie von den berechtigten Empfängern abgerufen werden können
- den „elektronischen Briefkästen", die als persönliche Speicher für Benutzer angeboten werden.

Der Zugriff zu diesen Dateien des Btx-Systems soll nur
- mit der persönlichen Kennung der Benutzer
- auf eindeutig zugeordnete Informationen möglich sein. Soll außer dem „Lesen" der Information eine weitergehende „Verarbeitung" möglich sein, ist dies ebenfalls im Berechtigungsumfang festzulegen (Authorization).

Die Datenbestände zur Verwaltung des Btx-Systems bestehen aus
- den Anschluß- und Teilnehmerdatensätzen
- den Vergütungssätzen, welche die Angaben über den beanspruchten Service enthalten (Telefongebühren und Entgelte).

Diese Datensätze sind dem Btx systemimmanent und werden von der Btx-Steuerung verwaltet.

3. Beim Anbieter (externer Rechner)

Ein Btx-Benutzer erhält über die Vermittlung des Btx-Systems Verbindung mit externen Rechnern, um an Anwendungen solcher, an das Btx angeschlossener Rechner, teilzunehmen. Es liegt ausschließlich in der Verantwortung des Betreibers des externen Rechners, vom Btx-Benutzer bestimmte Datensicherungsprodzeduren (z. B. anwendungsbezogene Kennung) zu fordern und mit den Mitteln des externen Rechners zu überwachen.

Kontrollmechanismen zur Sicherung von Daten im Btx

1. Feststellung (Identifikation)

Der Btx-Benutzer wird durch seine Geräte-Anschlußnummer identifiziert. Diese Nummer ist mit der Telefonnummer eines Telefonteilnehmers vergleichbar. In Verbindung mit dieser Nummer, die bei Installation eines Btx-Anschlusses zugeteilt wird, ist für den Benutzer der „Anschlußsatz" des Btx-Systems anzulegen. In diesem Anschlußsatz wird der Benutzer beschrieben und bei Nutzung der Möglichkeit der „Mitbenutzung" auch die Berechtigungsdaten der Mitbenutzer festgelegt. Dieser Datensatz des Benutzers steht ausschließlich dem Betreiber (Btx-Steuerung) zur Verfügung. Die in der Anlage zu § BDSG geforderten techn

Analyse der Gefahren angebotene Dienste	gespeicherte Daten	speichernde Stelle	Gefährdungspotential	Kenntnis des Betroffenen	Regelungen des BDSG
Mitteilungen an einzelne oder mehrere (electronic mail)	private und geschäftliche Mitteilungen	Betreiber (Deutsche Bundespost)	Offenbarung privater und geschäftlicher Geheimnisse Kommunikationsmatrix	wenig wahrscheinlich	nur, wenn in Dateien gespeichert § 9 Abs. 1 Speicherbefugnis § 14 Abs 2 Satz 2 Sperrung § 14 Abs. 3 Löschung
Abruf von Informationen (Seiten)	personenbezogene Daten (z. B. Biographien, Werbeaussagen)	Betreiber oder Anbieter (im externen Rechner)	Bekanntgabe an viele Teilnehmer	wahrscheinlich	wird vom BDSG nicht erfaßt, weil keine Speicherung in einer Datei
Teilnahme an Spielen	Angaben über den Teilnehmer (z. B. Name, Anschrift, Alter, Beruf)	Betreiber und Anbieter	Verwendung für andere Zwecke, z. B. Werbung größere Offenbarungsbereitschaft in häuslicher Umgebung	nein nein	Erhebung wird vom BDSG nicht erfaßt: bei Speicherung in Dateien: § 23 (weitgehende) Speicherbefugnis Einwilligung
Dienstleistungen externer Rechner	Angaben über den Teilnehmer Daten über das Nutzungsverhalten	Anbieter	Verwendung für andere Zwecke, z. B. Werbung Persönlichkeitsprofil Individualisierung bisher anonymer Vorgänge größere Bereitschaft in häuslicher Umgebung	nein nein wenig wahrscheinlich nein	Erhebung wird vom BDSG nicht erfaßt; bei Speicherung in Dateien: § 23 (weitgehende) Speicherbefugnis, Einwilligung § 27 Abs. 2 S. 2 Sperrung § 27 Abs. 3 Löschung
Bereitstellung aller Dienste	Angaben über den Teilnehmer: Daten über vermittelte Dienste Daten über abrechnungsrelevante Sachverhalte	Betreiber	Persönlichkeitsprofil	nein	fraglich, ob vom BDSG erfaßt; wenn Speicherung in Dateien: § 9 Abs. 1 Speicherbefugnis § 14 Abs. 2 Satz 2 Sperrung § 14 Abs. 3 Löschung

So regelt das Bundesdatenschutzgesetz die Risikovorbeugung bei der Datenspeicherung im Btx.

schen und organisatorischen Maßnahmen werden beim Betreiber erfüllt.

2. **Beurkundung (Verifikation)**

Die Beurkundung der Benutzer wird durch Verwendung eines persönlichen Kennwortes erreicht, dabei wird die dem Stand der Technik entsprechende Methode eingesetzt.

Bei jeder Anmeldung (sign-on) eines Btx-Benutzers am Btx-System erfolgt die Kennwortprüfung. Erst nach Gleichheit des eingegebenen Kennwortes mit dem im Teilnehmersatz des Benutzers gespeicherten persönlichen Kennwortes wird die Btx-Nutzung freigegeben.

Das persönliche Kennwort ist vom Benutzer selbst zu bilden. Er muß bei erstmaliger Btx-Nutzung nach einer ihm am Bildschirm aufgezeigten Prozedur ein Kennwort bilden und in das System eingeben. Dieses persönliche Kennwort kann vom Benutzer jederzeit, beliebig häufig geändert werden. Hierdurch wird erreicht, daß der Benutzer bei Verdacht einer Kennwortbekanntgabe oder vermutetem Versuch, sein Kennwort zu ermitteln, ein anderes Kennwort eingeben kann. Jeder Btx-Benutzer kann seinen Kennwortgebrauch selbst steuern.

Sollte ein Btx-Benutzer ein falsches Kennwort eingeben, wird er abgewiesen und erhält zwei weitere Versuche. Ist auch der dritte Kennworteingabeversuch nicht erfolgreich, wird die Verbindung zu Btx unterbrochen. Dieser Benutzer hat am gleichen Tag (24-Stunden-Zyklus) weitere 2 × 3 Kennworteingabemöglichkeiten. Ist auch der 9. Versuch nicht erfolgreich, wird der Btx-Anschluß gesperrt. Erst durch ein besonderes Verfahren (Postamt) kann der sich legitimierende Teilnehmer seinen Btx-Anschluß wieder aktivieren.

Analyse der Gefahren		Regelungen des Staatsvertrages generell:
	Art. 9 Abs. 1	subsidiäre Geltung des allgemeinen Datenschutzrechts
	Art. 9 Abs. 7	Rechte des Betroffenen
	Art. 9 Abs. 8	Verpflichtung zu Datensicherungsmaßnahmen
angebotene Dienste	Art. 10	Geheimhaltung
Mitteilungen an einzelne oder mehrere (electronic mail)	Art. 10	Geheimhaltung
	Art. 9 Abs. 4	Speicherung und Löschung der Verbindungs- und Abrechnungsdaten (§ 38b Abs. 5 Fernmeldeordnung, Löschung der Mitteilungen nach max. 60 Tagen)
Abruf von Informationen (Seiten)	Art. 9 Abs. 5	Btx-Angebot gilt als Datei Die für Übermittlungsvorgänge geltenden Vorschriften des Datenschutzes sind anzuwenden und vom Anbieter zu beachten
Teilnahme an Spielen Dienstleistungen externer Rechner	Art. 9 Abs. 6	Abfrage (= Erhebung) und Speicherung von Daten nur – soweit dies für das Erbringen der Leistung, den Abschluß oder die Abwicklung eines Vertrages erforderlich ist. Verarbeitung dieser Daten nur – im Rahmen der Zweckbestimmung des Vertrages oder der Leistung; darüber hinaus nur aufgrund Einwilligung Aufklärung über die Bedeutung der Einwilligung Mit Ausnahme der Kreditgeschäfte: Die Leistung, der Abschluß oder die Abwicklung eines Vertragsverhältnisses dürfen nicht von der Einwilligung abhängig gemacht werden. Einwilligung über Bildschirmtext wird nur nach Bestätigung wirksam.
	Art. 9 Abs. 8 Nr. 2	Sicherstellung, daß der Teilnehmer Daten nur durch eine bewußte und eindeutige Handlung übermitteln kann.
Bereitstellung aller Dienste	Art. 9 Abs. 2	Abfrage und Speicherung von Daten nur, soweit und so lange für – Vermittlung des Abrufs von Angeboten (Verbindungsdaten), – Abrechnung von Gebühren und Entgelten (Abrechnungsdaten) erforderlich.
	Art. 9 Abs. 3	Speicherung der Abrechnungsdaten nur mit Einverständnis des Teilnehmers in detaillierter Form. Übermittlung der Abrechnungsdaten nur aufgrund besonderer Rechtsvorschrift oder an den Anbieter zur Betreibung. Übermittlung der Verbindungsdaten unzulässig. Löschung der Abrechnungsdaten, wenn für Zwecke der Abrechnung nicht mehr erforderlich. Löschung der Verbindungsdaten nach Ende der jeweiligen Verbindung.
	Art. 9 Abs. 7 Satz 4	Anspruch des Betroffenen auf Löschung der Verbindungs- und Abrechnungsdaten.
	Art. 9 Abs. 8 Nr. 1	Sicherstellung, daß Verbindungsdaten gelöscht werden.

Analyse der Gefahren, die in den verschiedenen Diensten im Bildschirmtext auftreten können.