Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 77 (1986)

Heft: 3

Artikel: Die PTT-Betriebe und die Datensicherheit

Autor: Lutz, H. P. W.

DOI: https://doi.org/10.5169/seals-904154

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 12.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Die PTT-Betriebe und die Datensicherheit

H.P.W. Lutz

Im Zusammenhang mit der modernen EDV-Technik stellt sich immer dringender die Frage nach der Sicherheit und der Sicherung der über die Fernmeldenetze übermittelten Informationen. Die nachfolgenden Ausführungen sollen dazu beitragen, vor allem im Anwendungsbereich des Datennetzes Telepac allfällig vorhandene falsche Vorstellungen und Erwartungen aus dem Wege zu räumen bzw. eventuell bisher unbeachtet gebliebene Möglichkeiten und Massnahmen für die Datensicherheit aufzuzeigen.

En rapport avec la technique moderne du traitement électronique des données, la sécurité et la protection des informations transmises par les réseaux de télécommunication deviennent de plus en plus importantes. Par son exposé l'auteur veut contribuer à éliminer les fausses idées et expectatives éventuelles, principalement en ce qui concerne le réseau de données Télépac, et montrer certaines possibilités et dispositions pour la sécurité des informations, jusqu'ici négligées.

Vortrag anlässlich der Informationstagung «Sicherheitsaspekte in Datennetzen» der SVD[1] am 21. November 1985 in Biel.

[1] SVD, Schweizerische Vereinigung für Datenverarbeitung, Postfach 373, 8037 Zürich.

Adresse des Autors
H.P.W. Lutz, dipl. Ing. ETH, GD PTT, Sektion Datenübermittlung, Viktoriastrasse 21, 3030 Bern.

1. Grundlagen und Vorgaben

Im Zusammenhang mit der Problematik Sicherheitsaspekte in Datennetzen ist eine Rückbesinnung auf die rechtlichen Grundlagen sowie ein Blick auf die unternehmungspolitische Grundeinstellung der PTT-Betriebe notwendig, innerhalb derer sich diese bewegen und ihre Tätigkeiten im Bereich der Teleinformatik entwickeln.

Die folgenden Grundlagen finden hierbei Verwendung:

- Bundesverfassung
- Telefon- und Telegrafenverkehrsgesetz (TVG)
- Verordnungen zum TVG
- Kommunikationsleitbild PTT
- Unternehmungspolitische Grundsätze und Richtlinien PTT

Der Wortlaut der relevanten Artikel der Bundesverfassung, des Telefon- und Telegrafenverkehrsgesetzes sowie des Kommunikationsleitbildes PTT und der unternehmungspolitischen Grundsätze PTT, insbesondere über die Dienstleistungspolitik, sind in Tabelle II zusammengestellt. Spezielle Beachtung verdient hierbei der Grundsatz 5 des Kommunikationsleitbildes PTT, welcher lautet: Die PTT-Betriebe befassen sich im Kommunikationsbereich mit der Übermittlung von Informationen und nicht mit Inhalten.

Aus dieser Formulierung ist die Rollenverteilung bzw. die Abgrenzung der Verantwortlichkeiten zwischen den PTT-Betrieben und den Kunden bzw. den Lieferanten von Fernmeldematerial klar erkennbar. Diese Abgrenzung hat übrigens auch zum heute realisierten Betriebskonzept des Dienstes Videotex geführt: Im Normalfall sind die Informationen, die irgendwelche Informationsanbieter für diesen Dienst zur Verfügung stellen wollen, in privatwirtschaftlich betriebenen Datenbanken gespeichert, und die PTT-Betriebe verbinden lediglich den Informationsbezüger über ihre Fernmeldenetze mit der entsprechenden Datenbank des gewünschten Informationsanbieters. Diese Aufgabenteilung hat sich – dies darf man, rückblickend auf zwei Jahre Betriebsversuch, getrost feststellen – sehr gut bewährt, und zwar sowohl in technischer als auch in betrieblicher oder politischer Hinsicht.

Nebst diesen rechtlichen und operativen Vorgaben bestehen im technischen Bereich eine ganze Reihe weiterer Vorgaben in der Form von Grundforderungen, Pflichtenheften und Spezifikationen für Systeme und einzelne Komponenten in den Bereichen Vermittlung, Übertragung und (PTT-) Endgeräte, in denen die Aspekte der Datensicherheit gebührende Beachtung finden. Als Beispiel diene hierzu das damalige «Rahmenpflichtenheft für ein Datennetz mit Paketvermittlung EDWP» aus dem Jahre 1978, das die Grundlage für die Beschaffung der heutigen Hardware- und Software für Telepac war und worin konkrete Anforderungen bezüglich Ausfallwahrscheinlichkeiten, Fehlerhäufigkeiten und Dienstqualität dieses Datennetzes festgeschrieben worden sind.

Die heute bekannten Bitfehlerraten auf den Fernmeldenetzen sind aus Tabelle I ersichtlich.

Bitfehlerraten auf den Fernmeldenetzen — Tabelle I

Netz	Bitfehlerraten
Telefonnetz	
Wählnetz	$10^{-6}...10^{-4}$
Mietleitungen analog	$10^{-7}...10^{-5}$
Mietleitungen digital	$10^{-8}...10^{-6}$
Telexnetz	$10^{-6}...10^{-5}$
Telepac	
X.25 (Paketmodus)	$10^{-8}...10^{-6}$
X.28 (Zeichenmodus)	$10^{-6}...10^{-4}$

Tabelle II

Bundesverfassung

Art. 36 Das Post- und Telegrafenwesen im ganzen Gebiet im ganzen Umfang der Eidgenossenschaft ist Bundessache.

Die heutige Rechtsprechung schliesst das Telefon, den Telex sowie den technischen Teil von Radio und Fernsehen hierbei mit ein.

Telefon- und Telegrafenverkehrsgesetz

Art. 1 *Fernmelderegal*
Die PTT-Betriebe haben das ausschliessliche Recht, Sende- und Empfangseinrichtungen sowie Anlagen jeder Art, die der elektrischen oder radioelektrischen Zeichen-, Bild- oder Lautübertragung dienen, zu erstellen und zu betreiben.

Art. 4 *Leistungspflicht*
Wo sie die erforderlichen Einrichtungen besitzen oder dieses Gesetz deren Schaffung vorsieht, sind die PTT-Betriebe unter den Bedingungen dieses Gesetzes, der Telegrafen- und Telefonordnung sowie der Ausführungsbestimmungen, zu den darin vorgesehenen Leistungen gegenüber jedermann verpflichtet.

Art. 6 *Amtsgeheimnis*
Die mit telegrafen- oder telefondienstlichen Verrichtungen betrauten Personen dürfen über den Telegrafen- oder Telefonverkehr einer Person sowie über den Inhalt der telegrafendienstlichen Aufzeichnungen und der vermittelten Telefongespräche keine Mitteilungen an Dritte machen.

Kommunikationsleitbild PTT
(März 1982)

Das Kommunikationsleitbild soll eine Konzentration der Kräfte zur sinnvollen Nutzung und Förderung bestehender und zukünftiger Kommunikationsformen bewirken, mögliche interne und externe Konflikte lösen helfen und periodisch angepasst werden. Das Kommunikationsleitbild dient in erster Linie als Grundlage des unternehmerischen Handelns der PTT-Betriebe. Es stützt sich auf die nachfolgenden zehn Grundsätze, welche die Aufgaben und Haltung der PTT-Betriebe in der Gesellschaft verdeutlichen und abgrenzen sollen:

Grundsatz 1 Die PTT-Betriebe sind dem Gemeinwohl verpflichtet.

Grundsatz 2 Die PTT-Betriebe stellen die Versorgung des ganzen Landes mit einwandfreien Post- und Fernmeldeleistungen zu gleichen Bedingungen und auf wirtschaftliche Weise sicher.

Grundsatz 3 Die PTT-Betriebe erbringen ihre Leistungen auf der Basis des gesetzlichen Auftrages.

Grundsatz 4 Die PTT-Betriebe bewahren ihre organisatorische und wirtschaftliche Einheit.

Grundsatz 5 Die PTT-Betriebe befassen sich im Kommunikationsbereich mit der Übermittlung von Informationen und nicht mit Inhalten.

Grundsatz 6 Die PTT-Betriebe behalten die öffentlichen Netzwerke für die Übermittlung von Informationen in ihrer Verantwortung.

Grundsatz 7 Die PTT-Betriebe stellen den freien Zugang zu allen von ihnen angebotenen Kommunikationsmöglichkeiten sicher.

Grundsatz 8 Die PTT-Betriebe gewährleisten in ihrem Aufgabenbereich den Persönlichkeitsschutz.

Grundsatz 9 Die PTT-Betriebe betreiben eine fortschrittliche und soziale Personalpolitik.

Grundsatz 10 Die PTT-Betriebe sind sich bewusst, dass nicht alles, was technisch möglich und wirtschaftlich tragbar, auch gesellschaftlich erwünscht ist, und beurteilen daher die Entwicklung im Kommunikationsbereich ganzheitlich.

Unternehmungspolitische Grundsätze und Richtlinien der PTT-Betriebe
(Januar 1978)

Dienstleistungsangebot

Die PTT-Betriebe wollen ein auf die allgemeinen Bedürfnisse ausgerichtetes Dienstleistungsprogramm erfüllen; sie überprüfen dabei periodisch alle ihre Leistungen, um festzustellen, ob sie hinsichtlich Bedürfnis und Ausmass noch dem tatsächlichen Interesse der Allgemeinheit entsprechen.

Als öffentlicher Dienstleistungsbetrieb sind die PTT-Betriebe darauf bedacht, im Rahmen der gesetzlichen Leistungspflicht und unter Beachtung der staatspolitischen und volkswirtschaftlichen Bedeutung das Dienstleistungsangebot auf die allgemeinen Bedürfnisse auszurichten, indem sie

- im Rahmen der verfügbaren Mittel die Nachfrage nach Dienstleistungen bestmöglich erfüllen,
- neue Dienstleistungen einführen, wenn sie einem ausgewiesenen Bedürfnis entsprechen und für längere Dauer eine angemessene Rendite versprechen,
- für jede einzelne Dienstleistung die Entwicklung der Nachfrage verfolgen und den gesamten Dienstleistungsfächer nach betriebswirtschaftlichen Kriterien periodisch überprüfen,
- für jede einzelne Dienstleistung die Entwicklung des Kostendeckungsgrades verfolgen und defizitäre Dienstleistungen gegebenenfalls tariflich sanieren oder aufheben; dabei sind die Möglichkeiten des Ausweichens auf andere Dienstleistungen zu berücksichtigen.

2. Datenschutz und Datensicherheit

Bei der Problematik Sicherheitsaspekte in Datennetzen sind grundsätzlich zwei Bereiche klar voneinander zu unterscheiden, nämlich diejenigen des Datenschutzes und der Datensicherheit.

Der *Datenschutz* hat als Zielsetzung, jeden Missbrauch – ob beabsichtigt oder unbeabsichtigt – von manuellen und maschinellen Datenverarbeitungsmitteln zu verhindern und eine ordnungsgemässe Datenverarbeitung sicherzustellen. Im Zentrum der Datenschutzproblematik steht heute der Persönlichkeitsschutz, d.h. der Schutz der durch die Daten ausgedrückten Sachverhalte des realen Lebens, insbesondere bei Daten über Personen und deren Privatsphäre. Die Zielsetzungen für eine ordnungsgemässe Datenverarbeitung sind von den jeweils hierfür verantwortlichen Stellen bzw. Benutzern festzulegen und in die Tat umzusetzen. Allen Datenschutzregelungen liegen naturgemäss einige Grundsätze zugrunde, wie:

- Zweckbestimmung der Datensammlungen (Begründung),
- öffentliche und bekannte Grundlagen für die Führung von Daten-

sammlungen,
- Auskunfts- und Einsichtsrecht für direkt Betroffene,
- Berichtigungsrecht bei falsch oder unvollständig gespeicherten Daten,
- Datenverkehrsregelung (Regelung der Weitergabe geschützter Daten).

Die Methoden zur Gewährleistung des Datenschutzes und der Datensicherheit werden *Datensicherung* genannt; sie umfassen alle Massnahmen technischer und organisatorischer Art, um Daten vor Verfälschung, Fehlverarbeitung, Zerstörung, Entwendung oder unzulässiger Verwendung zu schützen. Der kombinierte Einsatz von Datensicherungsmassnahmen führt dann zur *Datensicherheit* und zum Datenschutz, wobei die erstere unabdingbare Voraussetzung für die Gewährleistung eines realen Datenschutzes ist.

Allen unzähligen Datensicherungsverfahren liegen ebenfalls einige Grundsätze zugrunde, wie:

- sinnvolle Redundanz gegen Datenverlust und -verfälschung,
- Abschirmung und Kontrolle gegen unzulässigen Datenzugriff,
- Trennung der Kompetenzen gegen Missbräuche durch Fachleute.

An technischen Möglichkeiten für die Datensicherung seien etwa folgende erwähnt, ohne dass hierbei auf die jeweilige technische Ausgestaltung im einzelnen eingegangen werden kann:

- Kanalcodierung,
- Fehlererkennungs- und Fehlerkorrektursysteme (Redundanzanreicherung),
- Informationsrückkopplung (Echoplex),
- Entscheidungsrückkopplung (ACK/NAK-Technik),
- zeichenweise Informationssicherung,
- blockweise Informationssicherung,
- zyklische Blocksicherung.

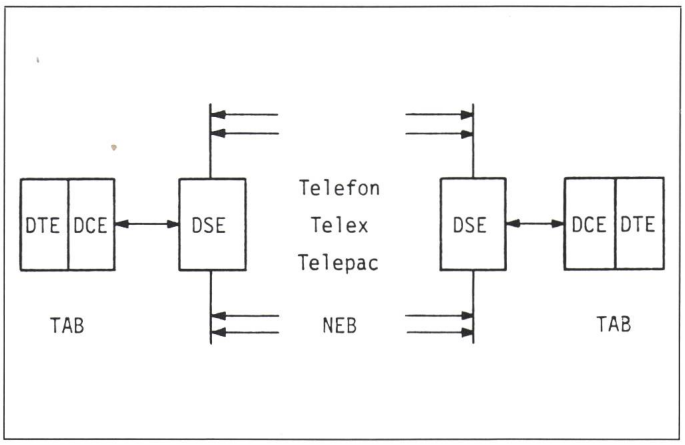
Alle diese technischen Massnahmen sind in der Regel durch den Benutzer in dessen Anwendungsprozeduren zu realisieren, wofür dieser auch die alleinige Verantwortung über deren Erfolg bzw. Misserfolg trägt.

3. Problematik Teilnehmeranschluss

Für die Datenübermittlung bieten die PTT-Betriebe ihren Kunden heute drei verschiedene Transportnetze mit entsprechenden Dienstleistungen an, nämlich:

Fig. 1
Prinzipschema eines Transportnetzes

TAB Teilnehmeranschlussbereich
NEB Netzbereich
DTE Data Terminal Equipment (Endgerät)
DCE Data Communication Equipment (Datenanschlussgerät)
DSE Data Switching Equipment (Vermittlungseinrichtung)



- das Telefonnetz (Wählnetz, Mietleitungen),
- das Telexnetz,
- das Datennetz Telepac.

Bezüglich der Sicherheitsaspekte sind alle drei Transportnetze einander ähnlich; sie lassen sich grundsätzlich wie in Figur 1 darstellen. Im *Netzbereich* bieten alle drei Transportnetze durch die jeweils eingesetzte Übertragungstechnik (Analogtechnik mit Trägerfrequenzsystemen oder Digitaltechnik mit Pulscode-Modulationssystemen) mit ihrer weitgehenden Multiplexierung eine sehr grosse Sicherheit gegen allfällige Beeinflussung des Leitungssignales durch Unbefugte. Ein möglicher Missetäter müsste demnach zunächst einmal dieselben Übertragungsausrüstungen einsetzen, um überhaupt an einen bestimmten Datenkanal heranzukommen; anschliessend müsste er Kenntnisse besitzen über Art und zeitlichen Ablauf der auf diesem Datenkanal abgewickelten Anwendung, um diesen Informationsfluss gezielt stören oder verändern zu können, und dies alles in Echtzeit. Dies stellt einen ganz erheblichen materiellen und finanziellen Aufwand dar, der wohl kaum so leicht und unbemerkt erbracht werden dürfte.

Der *Teilnehmeranschlussbereich* hingegen ist heute sicherheitsmässig als der schwächste Bereich in allen drei Netzen zu bezeichnen, wird doch jeder einzelne Anschluss dienstspezifisch zwei- oder vierdrähtig bis zum Teilnehmer geführt. Innerhalb der Hausinstallationen, die zudem weitverzweigt sein können, bestehen naturgemäss mannigfaltige Möglichkeiten der missbräuchlichen Anzapfung eines Datenkanals, auf die hier aber im einzelnen nicht näher eingegangen werden kann und die in der Regel nicht die PTT-Betriebe betreffen.

4. Datensicherheit im Datennetz Telepac

Die PTT-Betriebe haben in ihrem Datennetz Telepac zahlreiche Massnahmen technischer und organisatorischer Art eingeplant, um die Datensicherheit innerhalb ihres Einflussbereiches zu gewährleisten. Nachstehend sind vor allem jene Massnahmen in summarischer Weise aufgeführt, die im Vergleich zu Mietleitungen und deren Anwendungen von einiger Bedeutung sind.

1. Virtuelle Verbindungen, dynamische Multiplexierung: Anwendung der Technik der virtuellen (nicht physikalischen) Verbindungen und der dynamischen Multiplexierung gemäss den internationalen Normen für die Paketvermittlungstechnik.

2. Steuerung und Kontrolle des Datenflusses: Netzinterne Steuerung, Überwachung und nötigenfalls auch Korrektur des Datenflusses, und zwar getrennt für die beiden Netzbereiche Teilnehmeranschluss und interzentrale Verbindungen.

3. Anschlussklassen: Anwendung bestimmter Anschlussklassen (Tab. III) mit definierten Bitraten und Zugangsprozeduren für X.25-Anschlüsse (Paketmodus) und für X.28-Anschlüsse (Zeichenmodus).

4. Geschlossene Teilnehmergruppen: Möglichkeit der Bildung von Teilnehmergruppen mit einzeln festgelegten oder gar keinen Verkehrsbeziehungen zu anderen Teilnehmern.

5. Anschlussidentifikation: Möglichkeit für den Rufenden bzw. den Gerufenen, die Teilnehmernummer seines Partners übermittelt zu erhalten und zu überprüfen.

6. NUI und Passwort: Anwendung eines Sicherheitsmechanismus mit

Anschlussklassen im Datennetz Telepac Tabelle III

	Übertragungsgeschwindigkeit	Übertragungsverfahren	Betriebsverfahren
Basisdienste	2 400 bit/s 4 800 bit/s 9 600 bit/s 48 000 bit/s	seriell, synchron seriell, synchron seriell, synchron seriell, synchron	duplex duplex duplex duplex
Zusatzdienste	bis 300 bit/s bis 1200 bit/s	seriell, asynchron seriell, asynchron	duplex duplex

Network User Identification NUI und Passwort; keine Speicherung von Passworten im Netz, sondern fallweise Berechnung mittels Algorithmus und Vergleich mit Eingabe.

7. Transparentes Benutzer-Datenfeld: Möglichkeit der Verwendung des transparenten Benutzer-Datenfeldes (Datenbereich mit Benutzerinformation) für die Verschlüsselung der Daten sowie der Verwendung geeigneter Prozeduren nach den Anforderungen des Benutzers.

8. Zeitsperren: Notwendigkeit, bei X.28-Anschlüssen die Eingabe von NUI und Passwort innerhalb einer Minute abzuschliessen.

Alle diese Massnahmen zusammen mit PTT-internen betrieblichen und organisatorischen Massnahmen bewirken, dass das Datennetz Telepac als generelles Transportsystem für die Text- und Datenkommunikation bezüglich Datensicherheit einen recht hohen Standard gewährleistet, der von den beiden anderen Transportnetzen, dem Telefonnetz und dem Telexnetz, auch nicht nur annähernd erreicht wird.

5. Datensicherheit im Videotexdienst

Im Gegensatz zu den im vorangehenden Abschnitt beschriebenen Massnahmen liegt die Problematik der Datensicherheit bei Videotex etwas anders, indem hier, wie im ersten Kapitel dargelegt, die PTT-Betriebe lediglich die technische Infrastruktur bereitstellen und damit die Netzverantwortung wahrnehmen, die Informationsanbieter hingegen die Dienstleistungen und Informationen zur Verfügung stellen und dabei die Nutzverantwortung tragen.

Wie beim Datennetz Telepac können auch bei Videotex verschiedene Massnahmen zur Gewährleistung der Datensicherheit vorgekehrt werden.

5.1 Massnahmen im Verantwortungsbereich der PTT-Betriebe

Die PTT-Betriebe haben bei der technischen Ausgestaltung des Dienstes bereits verschiedene Vorkehrungen getroffen; die wichtigsten davon sind die folgenden:

1. Teilnehmernummer und Passwort: Anwendung eines Sicherheitsmechanismus für die richtige Zuordnung von Passwort zu entsprechender Teilnehmernummer.

2. Sperrung bei falscher Passworteingabe: Sperrung des Anschlusses bei der dritten falschen Eingabe eines Passwortes durch den Abonnenten.

3. Eingeschränkte Freigabe gesperrter Anschlüsse: Freigabe gesperrter Anschlüsse nur auf schriftliches Begehren des betroffenen Abonnenten.

4. Aufbau und Zuteilung der Passworte: Zuteilung des Passwortes mittels Zufallsgenerator mit minimaler Länge von 4 Zeichen; zusätzlich Hinweis an den Abonnenten, mehr als 4 Zeichen (Ziffern und Buchstaben) sowie keine leicht merkbaren Kombinationen (gleiche Ziffernfolgen, Geburtstage, Tagesdaten u.ä.) zu verwenden und das Passwort öfters zu wechseln.

Alle diese Massnahmen haben dazu geführt, dass in den letzten sechs Monaten seit ihrer Wirksamkeit keine Fälle von sog. Hackern (böswilliges Eindringen in Datenbanken unter Verwendung einer fremden Identifikation) mehr bekannt geworden sind.

5.2 Massnahmen im Verantwortungsbereich der Informationsanbieter

Es ist seit längerer Zeit bekannt, dass verschiedene Wirtschaftszweige Videotex nur bei erhöhter Sicherheit in ihre Dienstleistungen miteinbeziehen wollen. Insbesondere die Banken sind, sofern sie die Auflagen seitens des Bankgeheimnisses voll beachten wollen, auf zusätzliche Sicherheitsmechanismen angewiesen. In diesem Bereich sind wiederum verschiedene Möglichkeiten denkbar, die einzeln oder in Kombination untereinander angewendet werden können:

1. Identifikation des Kunden: Anwendung eines Sicherheitsmechanismus bei der Identifikation eines Kunden, der die Dienstleistungen z.B. einer Bank beanspruchen will, mit
- Vertragsnummer (durch Bank zugeteilt),
- Transaktionsnummer (durch Bank zugeteilt, nur einmalig verwendbar),
- Passwort (durch Kunden beliebig veränderbar).

2. Einsatz zusätzlicher Infrastruktur: Einsatz einer speziellen Sicherheits-Datenbank für die Verwaltung des Sicherheitsmechanismus (z.B. elektronische Schlüssel, evtl. mehrstufig) sowie gegebenenfalls Einsatz von Chiffriergeräten bei den Datenbanken und bei den Kunden der betreffenden Banken. Eine solche Sicherheits-Datenbank könnte durchaus mehreren Banken oder Unternehmen gleichzeitig dienen und müsste durch eine beauftragte private Trägerschaft betrieben werden.

Die technische Entwicklung in diesem Bereich ist bei weitem noch nicht abgeschlossen, und es ist mit Sicherheit zu erwarten, dass mit einem breiteren Einsatz der neuen sog. Memory-Cards (mit eingebautem Mikroprozessor) neue und noch zuverlässigere technische Lösungen zu erwarten sind.

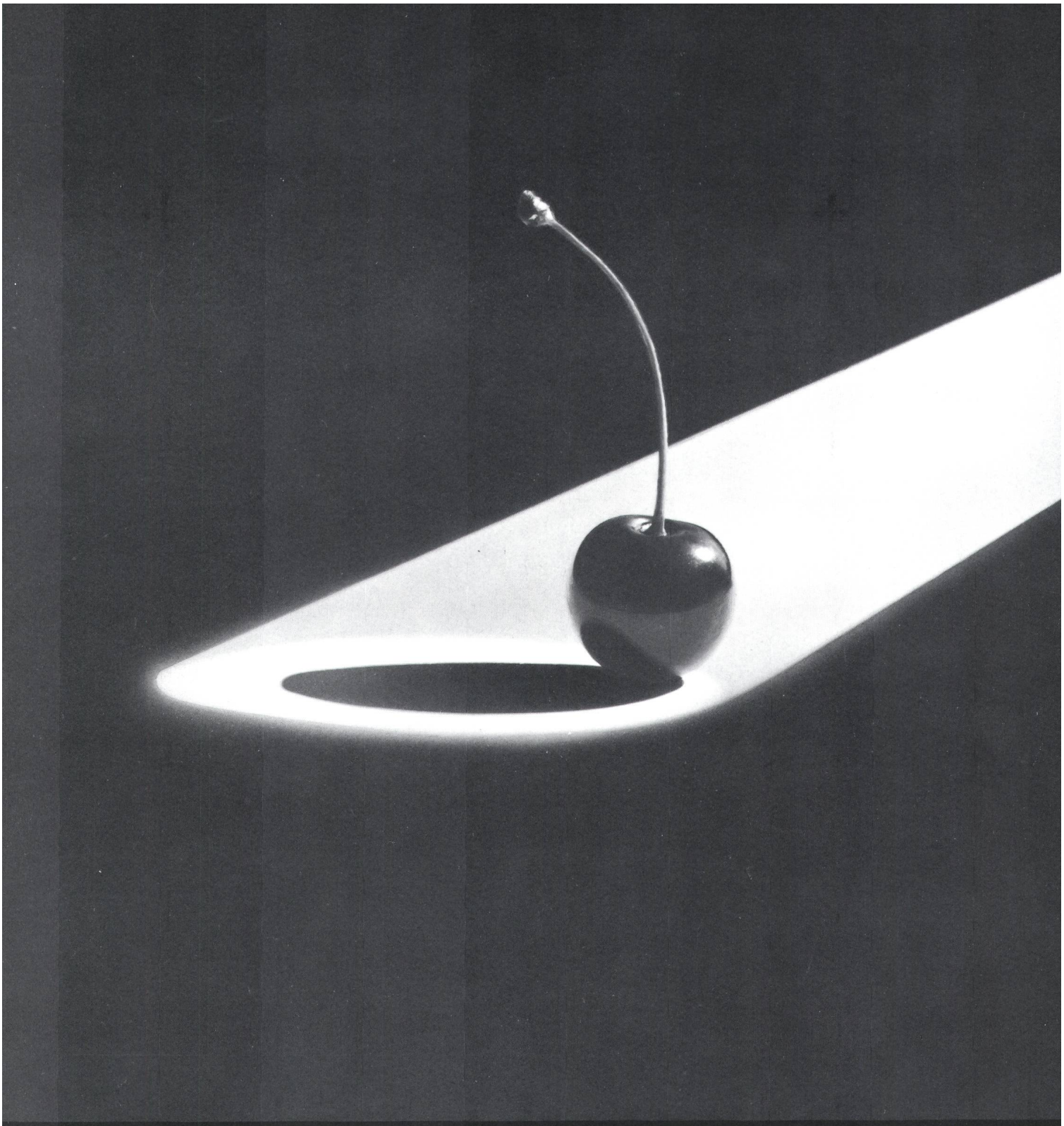
6. Schlussfolgerungen

Aus den bisher gemachten Ausführungen können die nachstehend aufgeführten Schlussfolgerungen abgeleitet werden:

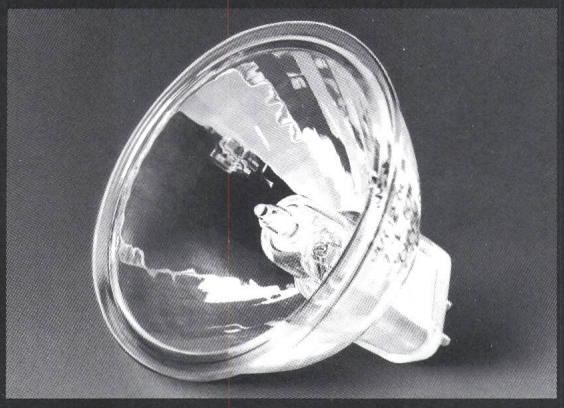
1. Das Datennetz Telepac bietet gegenüber dem Telefonnetz (Wählnetz und Mietleitungen) und dem Telexnetz eine erheblich grössere Sicherheit gegen missbräuchlichen Datenzugriff im Netz und bei Datenbanken.
2. Das Datennetz Telepac bietet gegenüber dem Telefon- und dem Telexnetz eine wesentlich bessere Unterstützung bei der Realisierung benutzerspezifischer Sicherheitsmassnahmen auf der Applikationsebene.
3. Ein umfassender Schutz der Daten bei deren Erfassung, Übermittlung und Verarbeitung ist mit vernünftigem technischem, organisatori-

schem und wirtschaftlichem Aufwand kaum je zu erreichen.

4. Für Anwendungen mit erhöhtem Sicherheitsbedürfnis sind unter Umständen geeignete Massnahmen zu treffen, die den unbefugten Datenzugriff auf der Teilnehmeranschlussleitung und den Hausinstallationen erschweren oder verunmöglichen.
5. Für Anwendungen im Bereich Videotex ist unter Umständen eine die geforderten Sicherheitsmechanismen verwaltende private Datenbank erforderlich, gegebenenfalls ergänzt durch Verschlüsselungsmechanismen bei den Datenbanken der interessierten Unternehmen und bei den Abonnenten.
6. Ein umfassendes Sicherheitskonzept muss sowohl Massnahmen im Bereich des Datenschutzes als auch solche im Bereich der Datensicherheit umfassen.
7. Für ein solches Sicherheitskonzept gibt es keine allgemein gültige Vorgehensweise; jeder einzelne Anwendungsfall muss unter Berücksichtigung aller Randbedingungen für sich allein betrachtet werden. Die verschiedenen Massnahmen sind aufeinander abzustimmen, um ein optimales Ergebnis zu erhalten.
8. Ein wirkungsvolles Sicherheitskonzept stützt sich ausnahmslos auf eine ausgewogene Kombination von geeigneten Massnahmen in den Bereichen Hardware, Software und Betriebsorganisation.



Alles kann Eindruck machen.



Hi-Light Tru-Aim®

Tungsten-Halogen Lampen für energiesparende Akzentbeleuchtung.

richtigen Licht hat sogar diese einfache rsche ihren dramatischen Auftritt!

Das richtige Licht heisst Hi-Light Tru-m, kommt von Sylvania und findet seinen nsatzbereich überall dort, wo Objekte zentuiert, wo dramatische Effekte erzielt erden sollen: in Auslagen, Schaukästen, useen, Läden, Wohnräumen und in der astronomie. Kurz, überall dort, wo lebens-he Farbwiedergabe und punktgerichtete strahlung Gestaltungselemente bilden.

Die kompakten Tru-Aim Halogen Lam-n zeichnen sich aus durch genaue Lichtlenkung, dank computerberechnetem Reflektor, hervorragende Farbwiedergabe, geringe Wärmeentwicklung (80% der Hitze wird rückwärts abgeleitet) und lange Lebensdauer (3000 Stunden) bei konstanter Leistung.

Hi-Light Tru-Aim Lampen bringen wesentlich mehr Lumen pro Watt als normale Displaylampen und sparen so bis zu 2/3 Energie.

Zusätzlich bietet Ihnen Sylvania diese Hochleistungslampen in 4 Farb-Versionen: rot, blau, grün und gelb. Eine neue Technologie ermöglicht es, das weiche farbige Punktlicht ungefiltert über die angestrahlten Objekte fliessen zu lassen. So wird das Gestalten mit Farbe einfacher und der erzielte Effekt eindrucksvoller.

SYLVANIA GTE

Gutes Licht. Besseres Licht.

GTE SYLVANIA AG
4, CH. DES LÉCHÈRES, 1217 MEYRIN, TEL. 022 82 00 72