Zeitschrift: Technische Mitteilungen / Schweizerische Post-, Telefon- und Telegrafenbetriebe = Bulletin technique / Entreprise des postes, téléphones et télégraphes suisses = Bollettino tecnico / Azienda delle poste, dei telefoni e dei telegrafi svizzeri

Herausgeber: Schweizerische Post-, Telefon- und Telegrafenbetriebe

Band: 64 (1986)

Heft: 9

Artikel: Qual è il contributo delle PTT all sicurezza dei dati?

Autor: Lutz, Hans Peter

DOI: https://doi.org/10.5169/seals-875045

Qual è il contributo delle PTT alla sicurezza dei dati?[1]

Hans-Peter LUTZ, Berna

Was tragen die PTT zur Datensicherheit bei?[1]
Zusammenfassung. *Der Einsatz der modernen EDV- und Prozessortechnik wird mehr und mehr mit der Anwendung verschiedenster Kommunikationsmittel verknüpft. In diesem Zusammenhang stellt sich – aus den verschiedensten Gründen – auch die Frage nach der Sicherheit und der Sicherung der über die Fernmeldenetze übermittelten Informationen. Dieser Artikel soll dazu beitragen, vor allem im Anwendungsbereich des Datennetzes Telepac allfällig vorhandene falsche Vorstellungen und Erwartungen aus dem Wege zu räumen bzw. bisher allenfalls unbeachtet gebliebene Möglichkeiten und Massnahmen für die Gewährleistung der Datensicherheit aufzuzeigen.*

Quel est l'apport des PTT à la sécurité des données?[1]
Résumé. *Les techniques modernes de l'informatique et des processeurs sont de plus en plus étroitement liées aux applications des moyens de communication modernes. C'est à ce propos – et pour diverses raisons – que se pose aussi la question de la sécurité et de la sauvegarde des données transmises par les réseaux de télécommunications. Par cet article, l'auteur souhaite contribuer à corriger les idées erronées et les espoirs trompeurs que l'on se fait notamment au sujet du réseau de données Télépac. Il montre aussi certaines possibilités et mesures éventuellement inédites en matière de protection des données.*

Riassunto. *La moderna tecnica di elaborazione elettronica di dati è sempre più impiegata per i più diversi mezzi di comunicazione. Sorge pertanto il problema della sicurezza e della protezione delle informazioni trasmesse attraverso le reti delle telecomunicazioni. Con questo articolo, l'autore vuole contribuire a eliminare, soprattutto riguardo alla rete di dati Telepac, opinioni e aspettative sbagliate e indicare possibilità e provvedimenti non ancora considerati in materia di sicurezza dei dati.*

1 Basi e premesse

Se si vogliono considerare i diversi aspetti del problema della sicurezza dei dati nelle reti di trasmissione è necessario richiamare alla memoria le basi giuridiche ed esaminare la politica aziendale svolta dalle PTT, in particolare la loro attività nel campo della teleinformatica. In questo contesto trovano applicazione:

- la Costituzione federale
- la legge sulla corrispondenza telegrafica e telefonica (LCTT)
- l'ordinanza di questa legge
- il modello di comunicazione delle PTT
- i principi e le direttive di politica aziendale delle PTT

Lo *specchietto 1* contiene gli articoli fondamentali della Costituzione federale e della legge sulla corrispondenza telegrafica e telefonica, lo *specchietto 2* i principi generali del modello di comunicazione e lo *specchietto 3* i principi di politica aziendale delle PTT concernenti l'offerta di servizi.

Particolare importanza va data al *principio 5 del modello di comunicazione delle PTT*:

> *Le PTT si occupano, nel campo della comunicazione, della trasmissione di informazioni e non del contenuto delle stesse*

Questo principio esprime chiaramente come sono distribuite le parti e delimitate le competenze tra Azienda delle PTT e utenti risp. fornitori di materiale delle telecomunicazioni. Del resto anche il concetto d'esercizio relativo al servizio Videotex è basato su questa delimitazione: normalmente, le informazioni messe a disposizione dai fornitori sono memorizzate in banche di dati a gestione privata e l'Azienda delle PTT, attraverso le sue reti di telecomunicazione, collega gli acquisitori di informazioni alla banca dati del fornitore richiesto. Questa ripartizione dei compiti ha dato buoni risultati sia dal punto di vista tecnico che da quello aziendale o politico.

Oltre a queste premesse di ordine giuridico e operativo, vi è, nel campo tecnico, una serie di altri presupposti in forma di esigenze di base, di capitolati d'oneri e di specificazioni per sistemi o singoli componenti, concernenti la commutazione, la trasmissione e i terminali (PTT), in cui gli aspetti della sicurezza dei dati sono tenuti in debito conto. Valga quale esempio il «Capitolato quadro per una rete di dati a commutazione di pacchetto

Specchietto 1

Costituzione federale

Art. 36 La posta e i telegrafi in tutta l'estensione della Confederazione sono del dominio federale

La giurisprudenza attuale include sotto il concetto di posta e telegrafi anche il telefono, il telex e la parte tecnica della radio e della televisione.

Legge sulla corrispondenza telegrafica e telefonica

Art. 1 Privativa delle telecomunicazioni

Il diritto di fare ed esercitare impianti per la spedizione ed il ricevimento, nonché impianti di qualsiasi natura, a scopo di trasmissione elettrica o radioelettrica di segnali, immagini o suoni, spetta esclusivamente all'Azienda delle poste, dei telegrafi e dei telefoni.

Art. 4 Obbligo di prestazione

Dove possiede gli impianti necessari, o dove la presente legge prevede la costruzione di essi, l'Azienda delle poste, dei telefoni e dei telegrafi è obbligata verso ognuno alle prestazioni contemplate dalla presente legge, dall'ordinanza sui telegrafi e telefoni nonché dalle loro prescrizioni esecutive.

Art. 6 Segreto d'ufficio

Alle persone incaricate di servizi telegrafici o telefonici è vietato di fare a terzi qualsivoglia comunicazione intorno alla corrispondenza telegrafica o telefonica di una persona, intorno al contenuto delle annotazioni di servizio loro affidate relative alla corrispondenza telegrafica e delle conversazioni telefoniche da esse trasmesse.

[1] Da una conferenza tenuta al congresso autunnale SVD 1985

Specchietto 2

Modello di comunicazione delle PTT

Il modello di comunicazione deve portare all'unione delle forze per l'utilizzazione razionale e l'incremento dei mezzi di comunicazione attuali e futuri, e contribuire a risolvere conflitti interni ed esterni; esso va adattato periodicamente. In primo luogo il modello di comunicazione serve da base all'attività aziendale delle PTT e poggia sui seguenti dieci principi, che definiscono e delimitano i compiti e il comportamento dell'Azienda delle PTT nella società.

Principio 1	Le PTT sono tenute ad operare per il bene comune
Principio 2	Le PTT assicurano all'intero Paese, a condizioni identiche e secondo principi economici, servizi ineccepibili delle poste e delle telecomunicazioni
Principio 3	Le PTT forniscono le loro prestazioni secondo il mandato conferito loro dalla legge
Principio 4	Le PTT intendono preservare la loro unità organica ed economica
Principio 5	Le PTT si occupano, nel campo della comunicazione, della trasmissione di informazioni e non del contenuto delle stesse
Principio 6	Le PTT detengono la responsabilità delle reti pubbliche che servono alla trasmissione delle informazioni
Principio 7	Le PTT assicurano il libero accesso a tutte le possibilità di comunicazione da loro offerte
Principio 8	Le PTT garantiscono, nel loro campo d'attività, la protezione della personalità
Principio 9	Le PTT praticano verso il personale una politica sociale e d'avanguardia
Principio 10	Le PTT sanno che non tutto ciò che è realizzabile dal lato tecnico ed economico è anche auspicabile sul piano sociale, pertanto considerano lo sviluppo nel settore della comunicazione sotto tutti i suoi aspetti.

Specchietto 3

Principi e direttive di politica aziendale delle PTT

Offerta di servizi
Per quanto concerne l'offerta di servizi, le PTT vogliono attuare un programma orientato ai bisogni del pubblico. Esse controllano perciò periodicamente se i loro servizi rispondono ancora di fatto, riguardo a necessità e portata, all'interesse pubblico.

Quale impresa di servizi pubblici, l'Azienda delle PTT tende, nel quadro dell'obbligo legale di prestazioni e in considerazione dell'importanza politica ed economica, a orientare la sua offerta di servizi ai bisogni del pubblico,

- soddisfacendo nel migliore dei modi la domanda di servizi, nei limiti dei mezzi a disposizione
- introducendo servizi nuovi solo se rispondono a un bisogno provato dell'utenza e se promettono una redditività adeguata per lungo tempo
- seguendo di ogni servizio l'evoluzione della domanda e rivedendo periodicamente, in base a criteri di economia aziendale, tutto il ventaglio dei servizi
- seguendo di ogni servizio l'evoluzione del grado di copertura dei costi, sanando, se del caso con misure tariffarie, o sopprimendo i servizi deficitari, tenendo sempre presente la possibilità di ripiegare su altri servizi.

EDWP» del 1978, che è servito da base per acquisire l'hardware e il software del servizio Telepac e che definisce concretamente le esigenze riguardo a probabilità di guasto, frequenza di errori e qualità di servizio di questa rete di dati.

2 Protezione dei dati e sicurezza dei dati

Per quanto concerne il problema della sicurezza dei dati nelle reti di trasmissione, si deve operare una netta distinzione tra *protezione* dei dati e *sicurezza* dei dati.

Lo scopo della *protezione* dei dati è di impedire ogni uso illecito – accidentale o intenzionale – dei mezzi manuali e automatici di elaborazione dei dati e di assicurare l'elaborazione regolare dei dati.

Attualmente al centro della problematica relativa alla protezione dei dati vi è la protezione della personalità cioè la protezione dei fatti della vita reale, in particolare delle persone e della sfera privata, espressi con i dati.

Per una elaborazione regolare dei dati, gli obiettivi devono essere fissati e realizzati dagli organi risp. dagli utilizzatori di volta in volta responsabili. Alla base di ogni regolamentazione in materia di protezione di dati vi sono alcuni principi ovvi come:

- la determinazione della destinazione delle raccolte di dati
- i criteri pubblici e conosciuti per la gestione delle raccolte di dati
- il diritto di chiedere informazioni e di prendere visione da parte di chi è direttamente interessato
- il diritto di rettifica in caso di dati memorizzati in modo inesatto o incompleto
- la regolamentazione del traffico di dati (regolamentazione della diffusione dei dati protetti)

I metodi atti ad assicurare la protezione dei dati sono definiti *tutela dei dati*; comprendono tutti i provvedimenti di natura tecnica ed organizzativa adottati per proteggere i dati da falsificazioni, errori di elaborazione, distruzioni, furti o usi illeciti. L'impiego combinato di diversi provvedimenti di tutela dei dati porta alla *sicurezza dei dati*, premessa indispensabile per garantire la protezione reale dei dati.

Anche alla base degli innumerevoli sistemi di sicurezza dei dati vi sono alcuni principi come:

- ridondanza adeguata per impedire perdite e falsificazioni dei dati
- difesa e controlli per impedire accessi non autorizzati
- ripartizione delle competenze per impedire abusi da parte di specialisti

Quali possibilità tecniche di tutela dei dati sono da menzionare, senza entrare nei particolari tecnici:

- la codifica di canale
- i sistemi di individuazione e correzione di errori (aumento della ridondanza)
- la retroazione delle informazioni (ecoplex)
- la retroazione delle decisioni (tecnica ACK/NAK)
- la protezione carattere per carattere dell'informazione
- la protezione a blocchi dell'informazione
- la protezione ciclica dei blocchi

Normalmente questi provvedimenti tecnici devono essere realizzati dall'utente nelle sue procedure d'applicazione; la responsabilità spetta dunque unicamente a lui.

3 Problematica collegamento d'utente

Per la trasmissione di dati, l'Azienda delle PTT mette a disposizione degli utenti tre diverse reti di trasporto e i relativi servizi:

- la rete telefonica (rete commutata, linee in locazione)
- la rete telex
- la rete dati Telepac

Per quanto concerne l'aspetto della sicurezza, le tre reti si assomigliano; nella *figura 1* sono rappresentate schematicamente.

Lato rete, la tecnica di trasmissione, di volta in volta adottata (analogica con sistemi a frequenze portanti o digitale con sistemi PCM), offre, con la relativa estesa multiplazione, una grande sicurezza, nelle tre reti, contro eventuali interferenze sul segnale di linea da parte di non autorizzati. Per potersi inserire su un determinato canale di dati, un eventuale intruso dovrebbe anzitutto servirsi degli stessi equipaggiamenti di trasmissione, poi, per disturbare o alterare con uno scopo preciso il flusso dell'informazione, dovrebbe sapere come e quando questo flusso si svolge sul canale di dati e tutto ciò in tempo reale. Sarebbe quindi necessario un impiego di mezzi materiali e finanziari tale da non poter passare inosservato.

Il lato più debole delle tre reti dal punto di vista della sicurezza resta invece il singolo *collegamento d'utente*, costituito, a seconda del servizio, da due o da quattro fili. Gli impianti domestici, con le loro diramazioni, offrono diverse possibilità di inserimento abusivo sui canali di dati, possibilità che in questa sede non sono trattate ulteriormente e che di regola non riguardano l'Azienda delle PTT.

4 Provvedimenti per garantire la sicurezza dei dati nella rete Telepac

L'Azienda delle PTT ha adottato nella rete dati Telepac diversi provvedimenti di natura tecnica e organizzativa atti a garantire la sicurezza dei dati nella sua sfera d'influenza. Nel seguito sono presentati sommariamente i provvedimenti che hanno una certa importanza per le linee in locazione e le relative applicazioni.

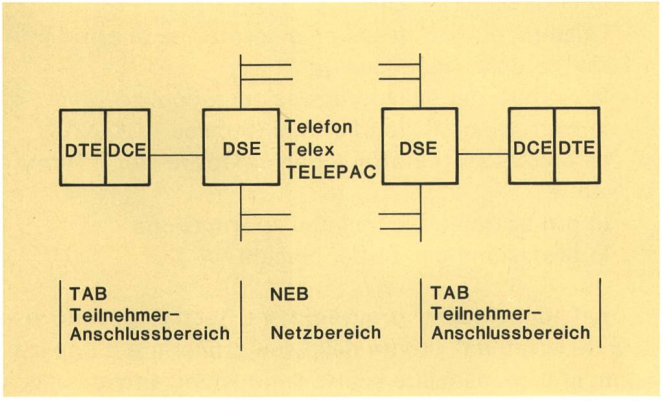

Fig. 1
Schema delle vie di comunicazione
Telefon – Telefono
DTE Apparato terminale di dati
DCE Apparato di terminazione del circuito di dati
DSE Apparato di commutazione di dati
TAB Lato collegamento d'utente
NEB Lato rete

41 Collegamenti virtuali, multiplazione dinamica

Trovano applicazione la tecnica dei collegamenti virtuali e la tecnica della multiplazione dinamica conformemente alle norme internazionali in materia di tecnica a commutazione di pacchetto *(tab. I)*.

Tabella I. Gerarchia multiplexer

Tipo	Canale singolo	Canale multiplo	Canale telefonico
MUX C	50 bit/s 300 bit/s	2,4 kbit/s	
MUX B	2400 bit/s 4800 bit/s 9600 bit/s	64 kbit/s	1
MUX A	64 kbit/s	2048 kbit/s	30
DMX-2	64 kbit/s	2,048 Mbit/s	30
DMX-8	2,048 Mbit/s	8,448 Mbit/s	120
DMX-34	8,448 Mbit/s	34,368 Mbit/s	480
DMX-140	34,368 Mbit/s	139,264 Mbit/s	1920
DMX-565	139,264 Mbit/s	565,992 Mbit/s	7680

42 Comando e controllo del flusso di dati

Il comando, la sorveglianza e se necessario anche la correzione del flusso dei dati sono interni alla rete e per di più separati lato collegamento d'utente e lato collegamenti intercentrali.

43 Classi di collegamento

Applicazione di determinate classi di collegamento con tassi di bit e procedure d'accesso ben definiti per collegamenti X.25 (modo a pacchetto) e X.28 (modo a caratteri), secondo le *tabelle II* e *III*.

44 Gruppi chiusi di utenti

Possibilità di formare gruppi di utenti senza relazioni di traffico verso altri utenti o con singole relazioni di traffico fisse verso altri utenti.

Tabella II. Classi di collegamento nella rete dati Telepac

Servizi di base		
Velocità di trasmissione	Sistema di trasmissione	Sistema d'esercizio
2 400 bit/s	Seriale, sincrono	Duplex
4 800 bit/s	Seriale, sincrono	Duplex
9 600 bit/s	Seriale, sincrono	Duplex
48 000 bit/s	Seriale, sincrono	Duplex
Servizi ausilari		
Velocità di trasmissione	Sistema di trasmissione	Sistema d'esercizio
Fino a 300 bit/s	Seriale, asincrono	Duplex
Fino a 1200 bit/s	Seriale, asincrono	Duplex

Tabelle III. Tasso d'errore dei bit sulle reti di telecomunicazione

Rete		Tasso d'errore dei bit
Rete telefonica	Commutata	$10^{-6} \ldots 10^{-4}$
	Linee in locazione analogiche	$10^{-7} \ldots 10^{-5}$
	Linee in locazione digitali	$10^{-8} \ldots 10^{-6}$
Rete telex		$10^{-6} \ldots 10^{-5}$
Telepac	X.25 (modo a pacchetto)	$10^{-8} \ldots 10^{-6}$
	X.28 (modo a caratteri)	$10^{-6} \ldots 10^{-4}$

45 Identificazione del collegamento

Possibilità del chiamante rispettivamente del chiamato di ricevere e di verificare il numero d'abbonato del proprio corrispondente.

46 NUI e parola chiave

Applicazione di un sistema di sicurezza mediante NUI (*N*etwork *U*ser *I*dentification) e parola d'ordine; nessuna memorizzazione di parole d'ordine nella rete, ma calcolo di volta in volta con algoritmo e confronto con l'immissione.

47 Campo di dati trasparente dell'utilizzatore

Possibilità di impiegare il campo dati trasparente dell'utilizzatore per la cifratura dei dati e di utilizzare procedure appropriate alle esigenze dell'utilizzatore.

48 Blocco a tempo

Per i collegamenti X.28, il NUI e la parola d'ordine devono essere immessi entro un minuto.

Grazie a tutto ciò e ai provvedimenti aziendali e organizzativi interni alle PTT, la rete dati Telepac, quale sistema di trasporto generale per la comunicazione di testi e di dati, garantisce, in quanto a sicurezza dei dati, uno standard assai elevato, dal quale la rete telefonica e la rete telex sono ancora molto lontane.

5 Conclusioni

Da quanto esposto si possono trarre le seguenti conclusioni:

1. Rispetto alla rete telefonica (rete commutata e linee in locazione) e alla rete telex, la rete dati Telepac offre un grado di sicurezza assai più elevato contro gli accessi illegali ai dati nella rete e nelle banche di dati.
2. Rispetto alla rete telefonica (rete commutata e linee in locazione) e alla rete telex, la rete dati Telepac si presta molto meglio all'adozione, a livello di applicazione, di misure di sicurezza specifiche per ogni utilizzatore.
3. Con mezzi tecnici, organizzativi ed economici normali è praticamente impossibile conseguire la protezione completa dei dati durante il loro rilevamento, la loro trasmissione e il loro trattamento.
4. Per le applicazioni che richiedono un grado di sicurezza più elevato occorrono provvedimenti che rendono eventualmente più arduo o impossibile l'accesso non autorizzato ai dati sulle linee d'utente e sugli impianti domestici.
5. Un concetto di sicurezza completo deve contenere sia misure di protezione dei dati che misure di sicurezza dei dati.
6. Non esiste un concetto di sicurezza valido per tutti i casi; per ottenere un risultato ottimale, occorre esaminare caso per caso, tenendo conto di tutte le condizioni marginali, e armonizzare di volta in volta tra di loro i diversi provvedimenti.
7. Un concetto di sicurezza efficace è fondato esclusivamente su una combinazione equilibrata di appropriati provvedimenti lato hardware, software e organizzazione dell'esercizio.