Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

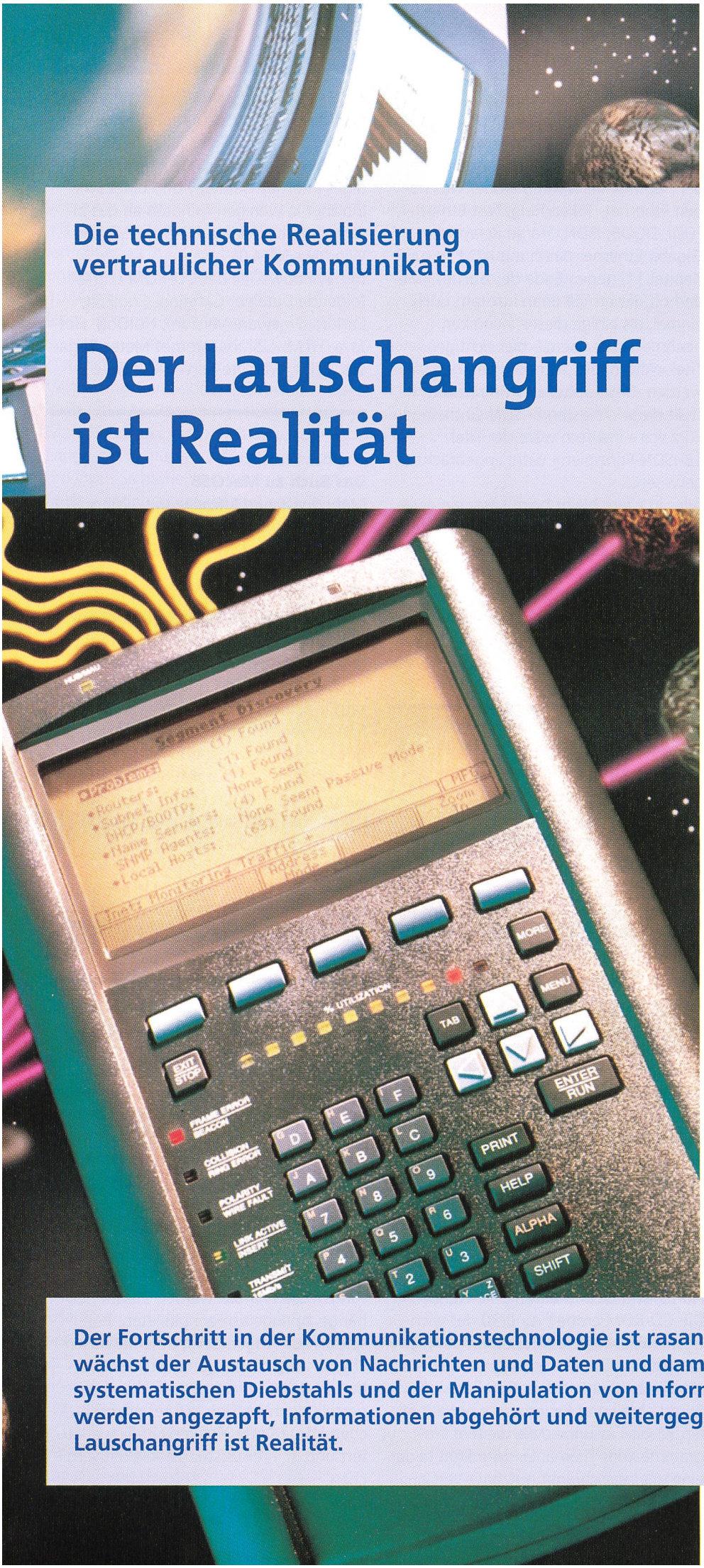
Band: 75 (1997)

Heft: 12

Artikel: Der Lauschangriff ist Realität

Autor: Hechfellner, Kurt

DOI: https://doi.org/10.5169/seals-876986



Die technische Realisierung vertraulicher Kommunikation

Der Lauschangriff ist Realität

Im Fadenkreuz der Lauscher stehen Konzerne und Forschungseinrichtungen, Behörden und innovative Unternehmen, Banken und Versicherungen sowie deren Kunden. Nur mit technischen Einrichtungen in Form von Verschlüsselungsgeräten für Sprache, Fax und Daten können Vertraulichkeit und Integrität in der Kommunikation realisiert werden.

KURT HECHFELLNER,
UNTERSCHLEISSHEIM

Anforderungen von Endanwendern und Netzbetreibern

Die Basis für jede technische Sicherheitsmassnahme ist zunächst die zum Einsatzzeitpunkt bestehende Kommunikationslandschaft. Um aber eine Investition in Sicherheitstechnologie auch für die Zukunft abzusichern, müssen nicht nur die zurzeit eingesetzten Kommunikationseinrichtungen, sondern auch deren absehbare technische Entwicklung berücksichtigt werden. Die Trends der Informations- und Kommunikationstechnologie, insbesondere die der Netze, sind daher von grösster Bedeutung:

- Die Liberalisierung und Deregulierung im weltweiten Telekommunikationsmarkt führt zu einer Vielzahl von Netzbetreibern, die sehr häufig global tätig sind.
- Netzstrukturen werden flacher, flexibler, und die Intelligenz der Netze steigt.
- Daten- und Sprachnetze wachsen zusammen.

Der Fortschritt in der Kommunikationstechnologie ist rasant. National wie international wächst der Austausch von Nachrichten und Daten und damit auch die Gefahr des systematischen Diebstahls und der Manipulation von Informationen. Datenleitungen werden angezapft, Informationen abgehört und weitergegeben – der ungesetzliche Lauschangriff ist Realität.

- Die Mobilnetze gewinnen massiv an Bedeutung sowohl in der Anzahl und der Applikationsvielfalt als auch hinsichtlich ihrer globalen Vernetzung.
- Satellitennetze werden weltweit neue Massstäbe setzen.
- Firmeninterne Netze für den gesamten Informationsaustausch im Unternehmen, sogenannte Corporate Networks, werden zunehmend eingesetzt, und dies unabhängig von der Firmengrösse.

Um die richtigen Informationssicherheitsmassnahmen zu ergreifen, muss zuerst die Frage beantwortet werden, welche Informationen in unserem Unternehmen geschützt werden müssen. Generell kann gesagt werden, dass alle Informationen schützenswert sind, die dem Unternehmen im Falle der Bekanntgabe an eine böswillige Person schaden können. Nicht nur wichtige Ausschreibungen oder Ergebnisse von Vertragsverhandlungen, sondern auch das vielfach intern weit gestreute Know-how eines Unternehmens ist schützenswert. Schützenswertes gibt es in allen Wirtschaftszweigen und Branchen.

Der Kreis der Interessenten an vertraulicher Information reicht vom Wettbewerber über den frustrierten Mitarbeiter bis hin zu verbrecherischen Organisationen und Terroristen.

Das Ziel der Massnahmen zur Informationssicherheit im Unternehmen ist letzten Endes die Erhaltung der Wettbewerbsfähigkeit. Ein zusätzlicher Teilaspekt, der oft übersehen wird, ist der Schutz der persönlichen Sicherheit der Vorstände in Grossunternehmen sowie der Personen im öffentlichen Bereich, wie beispielsweise Politiker. Schutzbedürftig sind hier zum Beispiel alle Informationen, die Rückschlüsse auf Aufenthaltsorte und Reisewege geben könnten.

Die genannten Anforderungen und Aspekte gelten primär für Endanwender. Sie gelten aber auch für Netzbetreiber und Dienstleistungsunternehmen, die im Interesse ihrer Kunden die Informations- und vor allem die Kommunikationssicherheit gewährleisten müssen. Wer das Leistungsmerkmal «Sicherheit» nicht bieten kann, wird mittelfristig nicht überleben können.

Leider müssen wir heute immer noch feststellen, dass der Nutzungsgrad auch fast als selbstverständlich geltender Massnahmen oft gering ist. Die Anstrengungen zur Verbesserung der Informationssicherheit müssen und werden deshalb weiter zunehmen.

Die grössten Probleme bei der weiteren Verbesserung liegen im fehlenden Bewusstsein und in einer nicht ganz richtigen Priorisierung der Investitionsmittel: Wer würde auf Schliessanlagen oder auf Bewachung bei den Eingängen zum Firmengelände verzichten mit der Begründung, dass es unwahrscheinlich sei, dass jemand sich einen unrechtmässigen Zutritt verschafft? Die Informationen, die auf den Kommunikationswegen übertragen werden, sind ähnlich ungeschützt wie ein von jedermann zugängliches Firmengelände.

Verschlüsselungskonzepte End-zu-End und Trunk

Bei der Realisierung der Informations- und Kommunikationssicherheit ist es unerlässlich, dass schon im ersten Schritt das oberste Management im Unternehmen einbezogen wird. Bedrohungen müssen auf dieser Ebene ernst genommen und für den Fortbestand des Unternehmens als wichtige funktionsübergreifende Aufgabe gesehen werden. Ohne diese Einsicht als feste Grundlage für den nächsten Schritt, die Sicherheitsanalyse, droht das Thema spätestens dann zu scheitern, wenn die Kosten für die Massnahmen bekannt sind.

Wenn wir den Kommunikationsweg der vertraulichen Informationen betrachten – vom Endgerät aus über Übertragungswege und Telekommunikationsanlagen innerhalb des Firmengeländes bis zum öffentlichen Bereich mit seinen eigenen Übertragungsstrecken und Vermittlungsanlagen – wird die erste Überlegung sein, wo die Verschlüsselung einzusetzen ist. Hier kommen grundsätzlich zwei Lösungsmethoden zum Einsatz, die End-zu-End-Verschlüsselung und die Trunk-Bündel- oder Linkverschlüsselung.

Die *End-zu-End-Verschlüsselung* bedeutet eine Verschlüsselung zwischen zwei Endgeräten. Endgeräte können Telefone, Faxgeräte, aber auch PCs, Rechneranlagen oder Kommunikationsserver sein. Auf der gesamten Übertragungsstrecke wird hiermit ein sehr wirksamer Schutz gegen Abhören und Manipulation erreicht. Die Teile des Übertragungsweges, die auf dem Firmengelände laufen, sind mit dieser Methode auch gegen sogenannte Innentäter geschützt. Der Nachteil liegt darin, dass jedes zu schützende Endgerät eine eigene Verschlüsselungseinrichtung benötigt.

Die *Trunk- oder Bündelverschlüsselung* kann dort eingesetzt werden, wo der Übertragungsweg das Firmengelände verlässt und im öffentlichen Bereich weitergeführt wird, beispielsweise nach der Telekommunikationsanlage oder nach dem Kommunikationsserver. Diese Methode kann allerdings nur an fest geschalteten externen Verbindungen zwischen verschiedenen Firmenstandorten eingesetzt werden. In diesem sogenannten «Corporate Network» kann mit Hilfe von Bündelverschlüsselungsgeräten der gesamte firmeninterne Informationsaustausch für externe Abhör- und Manipulationsversuche wirksam geschützt werden. Der Nachteil dieser Methode ist, dass innerhalb des Firmengeländes selbst kein Schutz vorhanden ist.

Ob End-zu-End-Verschlüsselung, Bündelverschlüsselung oder eine Kombination daraus sinnvoll ist, hängt vom jeweiligen Einsatzfall ab. Es müssen hier das Schutzbedürfnis, die eigene Kommunikationslandschaft sowie die örtlichen Gegebenheiten berücksichtigt werden. Das wichtigste ist, dass die Information bei der Übertragung genau dort geschützt ist, wo es am leichtesten und unauffälligsten ist, sie abzuhören. Dies ist der Fall sowohl bei leicht zugänglichen Verteilerschränken als auch bei den öffentlichen Richtfunk- und Satellitenstrecken.

Technische Realisierung der Sprach-, Fax- und Datenverschlüsselung

Für die Verschlüsselung bei den unterschiedlichen Kommunikationsdiensten stellt Siemens eine Familie von Verschlüsselungsgeräten zur Verfügung, die DSM-Familie (DSM: Datensicherungsmodul). Gemeinsam für alle Geräte der DSM-Familie gilt:

- eigenständige Verschlüsselungseinheit mit standardisierter Schnittstelle nach ITU-T
- kein Eingriff in die schon vorhandene Kommunikationslandschaft
- einfache Installation und Bedienung
- vollautomatisches Schlüsselmanagement für den Benutzer

Sprachverschlüsselung

Die Sprachkommunikation ist nach wie vor ein sehr häufig genutztes Medium, über das allzuoft äusserst vertrauliche Informationen ausgetauscht werden. Die Verschlüsselung der Sprache ist damit ein äusserst wichtiges Element in der Palette der Informationssicherheit. Die einzige heute weltweit verfügbare Schnittstelle

für ein Sprachverschlüsselungsgerät ist die analoge Schnittstelle (oder a/b-Schnittstelle). Die Spezifikation dieser Schnittstelle kann sich von Land zu Land geringfügig ändern, ist jedoch im Prinzip gleich und bekannt. ISDN und darin die digitale SO-Schnittstelle ist zwar bereits weit verbreitet, die weltweite Verfügbarkeit eines transparenten ISDN-Kanals ist jedoch noch nicht gewährleistet.
Aus diesem Grund hat Siemens entschieden, unter anderem ein Verschlüsselungsgerät für den analogen Sprachkanal zu entwickeln. Dieses Gerät kann über einen Terminaladapter auch an ISDN-Netze angeschlossen werden, ein weltweiter Einsatz dieses Sprachschlüsselgerätes ist damit gewährleistet.
Die technische Lösung für das Sprachschlüsselgerät sieht wie folgt aus: Auf der Telefonseite befindet sich ein Vocoder (Sprachkodierer), der die analoge Sprache digitalisiert und komprimiert und somit die Voraussetzung für die digitale sichere Verschlüsselung schafft. Die Verschlüsselung (im darauffolgenden Kryptoteil) ist manuell durch eine Taste aktivierbar. Diese Taste ist zusammen mit einer Chipkarte, in der die Schlüsselinformationen sowie die Funktionen für den Schlüsselaustausch gesichert gegen Auslesen und Veränderung gespeichert sind, das einzige Bedienelement für den Anwender. Nach dem Verschlüsselungsteil wird ein herkömmliches Modem benutzt, um die verschlüsselten digitalen Signale für die Übertragung auf der analogen Leitung umzusetzen.
Das Verschlüsselungsgerät wird einfach zwischen Telefon und Netz, am Hauptanschluss oder über eine Telekommunikationsanlage, eingeschleift. Unter der Voraussetzung, dass ein entsprechendes Gerät auch beim Partner installiert ist, kann bei Bedarf damit die Sprachinformation auf der gesamten Übertragungsstrecke verschlüsselt werden.

Faxverschlüsselung

Faxübertragungen sind besonderen Gefahren ausgesetzt. Ein sehr häufiges Problem sind die ungewollten Fehlleitungen, die – anders als bei Telefongesprächen – meist nicht vor oder während der Übertragung zu erkennen sind.
Das Faxverschlüsselungsgerät ist als Ergänzung zum Faxgerät die optimale Lösung für die sichere Übertragung von Dokumenten. Es kann an das öffentliche Telefonnetz oder an private Telefonanlagen angeschlossen werden und kommuniziert mit allen Faxgeräten der Gruppe 3 nach ITU-T. Die Authentisierung der Teilnehmer erfolgt sehr einfach und komfortabel mittels der Chipkarte.
Ganz bewusst wurde das Faxverschlüsselungsgerät als Ergänzungsmodul für Faxgeräte konzipiert, damit den Anwendern die Vorteile ihrer bestehenden Infrastruktur voll erhalten bleiben. Das heisst vor allem, dass das vorhandene Faxgerät keine wertlose Investition ist, wenn zur Sicherung der Dokumentenübertragung ein Verschlüsselungsgerät installiert wird. Genauso kann bei Bedarf jederzeit das alte Faxgerät gegen ein neues Modell ausgetauscht werden, ohne dass das Faxverschlüsselungsgerät dadurch wertlos wird.
Die Authentisierung des Senders und des Empfängers sowie die Datenverschlüsselung während der Übertragung erfolgen automatisch. Für die Verschlüsselung der Bildinformation einer Faxnachricht wird pro Übertragung ein geheimer Schlüssel, der sogenannte Sitzungsschlüssel, neu erwürfelt. Dieser wird zwischen den mit dem Faxverschlüsselungsgerät ausgestatteten Teilnehmern mit Hilfe des individuellen Schlüssels des Benützers im Public-Key-Verfahren ausgetauscht. Der individuelle Schlüssel ist auf der Chipkarte gespeichert und ist dort mit Hilfe einer nicht veränderbaren elektronischen Unterschrift gesichert. Wenn die Chipkarte nicht eingeschoben ist, erlaubt das Faxverschlüsselungsgerät dem Benutzer das unverschlüsselte Senden von Faxdokumenten. Das Gerät ist ausserdem immer für den unverschlüsselten Empfang bereit. Dadurch wird die Erreichbarkeit aller Faxteilnehmer gewährleistet.

Paketverschlüsselung

Für öffentliche und private Paketnetze auf Basis von X.25 nach ITU-T wurde ein Paketverschlüsselungsgerät entwickelt. Es wird einfach – genau wie die anderen Geräte der DSM-Familie – in die Leitung zwischen Teilnehmerendgerät (PC, Kommunikationsserver, Host usw.) geschaltet und bietet einen netzübergreifenden Schutz der vertraulichen Informationen. Verschlüsselt werden hierbei nur die Nutzdaten; Signalisierungen und Adressen bleiben unverschlüsselt.
Das Gerät schützt bei Datenübertragungen vor unbefugten Zugriffen und vor Manipulationen im Netz. Erreicht wird dies durch eine sichere Teilnehmeridentifikation und die Zugangskontrolle vom und zum Netz. Grundsätzlich kommen nur solche Verbindungen zustande, die der Sicherheitsoperator für seine Benutzergruppe zugelassen hat. Die Möglichkeit der unverschlüsselten Kommunikation mit bestimmten, vom Sicherheitsoperator zugelassenen Teilnehmern ohne Schlüsselgerät bleibt dabei selbstverständlich erhalten.
Ein komfortables Schlüsselmanagement über eine Sicherheitszentrale erlaubt es dem Anwender, die Verschlüsselungsgeräte zentral und gesichert über das X.25-Netz zu steuern.

Trunkverschlüsselung für Daten

Um einen sicheren Schutz von kontinuierlichen Datenströmen zu gewährleisten, kann ein entsprechendes Trunk- oder Bündelverschlüsselungsgerät eingesetzt werden. Dieses Gerät verschlüsselt Datenströme unterschiedlicher Bitraten, die über angemietete Übertragungsstrecken oder innerhalb eines Vermittlungsnetzes transportiert werden. Gerade bei umfangreichen Netzen, wie sie von privaten und öffentlichen Anbietern oder Grossunternehmen (Corporate Networks) unterhalten werden, bietet das Trunkverschlüsselungskonzept optimalen Schutz vertraulicher Daten.
Das Verschlüsselungsgerät arbeitet grundsätzlich transparent und vollautomatisch an synchronen Standleitungen mit Geschwindigkeiten bis zu 2 Mbit/s. Varianten für die gängigen Schnittstellen V.241 V.35, V.36, X.21 sowie für PCM-Struktur nach G.703/704 (E1/T1) sind erhältlich.
Initialisierung, Schlüsselwechsel und eine umfassende Betriebsüberwachung erfolgen im Dialog mit der Sicherheitszentrale, vorzugsweise über X.25-Verbindungen mit Absicherung durch das Public-Key-Verfahren. Die Verbindungen zwischen der Zentrale und den Verschlüsselungsgeräten bilden ein logisches Managementnetz, das jedoch physikalisch auch über die mit den Trunkschlüsselgeräten gesicherten Strecken geführt werden kann.
Auch hier ist die Chipkarte ein wesentlicher Bestandteil des Sicherheitskonzepts. Die Chipkarte dient hier zur Authentisierung des Verschlüsselungsgeräts gegenüber der Sicherheitszentrale und zur Sicherung der Kommunikation zwischen den Systemeinheiten.

Schlüsselmanagement

Chipkarten sind ein wesentlicher Bestandteil des Schlüsselmanagementkon-

zeptes. Auf diesen Karten sind alle sicherheitsrelevanten Daten unauslesbar gespeichert. Weiterhin befindet sich dort das für die Bearbeitung der sicherheitsrelevanten Vorgänge erforderliche Prozessorsystem inklusive Krypto-Koprozessor. Die hierarchische Sicherheitsstruktur ermöglicht eine sehr einfache Bedienung am Gerät und gleichzeitig eine hohe Flexibilität bei der Parametrisierung des Gesamtsystems.
Die Benutzerkarte, die als einzige Karte für die Bedienung des Verschlüsselungsgeräts notwendig ist, beinhaltet alle Funktionen für den sicheren Schlüsselaustausch. In dieser Hinsicht kann die Chipkarte als ein eigenständiges komplettes Schlüsselgerät gesehen werden, das den jeweiligen Sitzungsschlüssel für die Nutzdatenverschlüsselung im Grundgerät bereitstellt.
Die Installationskarte hat die Aufgabe, das Verschlüsselungsgerät für den Betrieb vorzubereiten, indem sie einen Installationsvorgang im Dialog mit dem Schlüsselgerät durchführt. Die Parametrisierung des Systems wird durch die dafür besonders vorbereitete Installationskarte erreicht. Parameter können hier beispielsweise geschlossene Benutzergruppen, unterschiedliche Kontroll-, Steuer- und Sicherheitsstufen sein.
Die Chipkarten werden durch eine Personalisierungseinheit, ein sogenanntes Trust Center personalisiert. Durch diese Personalisierung unter der Verwendung von Mechanismen der elektronischen Unterschrift wird die Authentizität der Chipkarten, der Schlüsselgeräte und der Kommunikationspartner untereinander sichergestellt.
Das Trust Center, das nur in einer vertrauenswürdigen und abgesicherten Umgebung zu betreiben ist, hat folgende Aufgaben:
- Personalisierung der Benutzer- und Installationskarten (Erst- oder Ersatzbereitstellung). Erzeugung eines individuellen Public-Key-Schlüsselpaares für jede Benutzerkarte
- Programmierung von Steuerfunktionen auf der Installationskarte für besondere Anwendungen
- Authentisierung der Daten auf jeder Chipkarte durch eine elektronische Unterschrift

Summary

Technical implementation of confidential communication

Encryption devices that can be used for end-to-end protection and on trunks (transmission links) have standardized interfaces, require no modifications to the terminal equipment to be protected and can, therefore, be easily integrated into the communications environment. In addition, they are very easy to operate, especially since the key management is fully automatic.
The overall security in the network requires that in future standards greater attention be given to the security of the information. In addition, the requirements for software functions that are critical to the security must be modelled on the requirements for correct and certified software.

Sicherheit in Netzen

Mit den vorher aufgezeigten Massnahmen ist nur ein Teilaspekt der Sicherheit in Netzen angesprochen worden. Der Themenkomplex Sicherheit in Netzen umspannt die Gesamtheit aller Netzkomponenten und Netzelemenente, die sich mit dem Transport und der Verarbeitung von Informationen im Netz befassen.
Dazu gehören:
- Sicherheit im Übertragungskanal.
- Netzübergänge bei verschlüsselten Diensten. Dieses Thema birgt erhebliche Probleme in sich, nicht zuletzt deshalb, weil im Rahmen der Standardisierung Informationssicherheitsaspekte nicht gebührend berücksichtigt wurden. Man denke hier an ein klassisches Problem, den Übergang von EURO-ISDN mit 64 kbit/s auf das US-ISDN mit 56 kbit/s. Dieser Übergang bzw. eine Conversion ist für den unverschlüsselten Sprachdienst standardisiert. Für einen verschlüsselten Sprachdienst ist derzeit noch keine Lösung in Sicht.
- Für die sichere Faxübertragung muss beim Verbindungsaufbau auch die Möglichkeit der Schlüsselübertragung gegeben sein. Derzeit ist in den standardisierten Protokollen dafür kein Raum vorgesehen.
- Ein weiterer Aspekt ist die Sicherheit gegen Missbrauch oder Fehlbedienungen von Netzeinrichtungen wie Vermittlungen und Router.

Typische Beispiele sind:
- der Zugriff auf die Fernwartungsschnittstelle einer Vermittlung über verschlüsselte Datenstrecken
- gesicherte Zugriffsverfahren auf das Netzmanagement
- Gebührenabrechnung durch Authentisierung und kryptographische Protokolle unter Nutzung von Chipkarten
- die Beweisbarkeit und die Aufzeichnungen von Änderungen und Manipulationen an wichtigen Einrichtungen durch Führen eines elektronischen Logbuches

- Als letztes in dieser sicherlich noch unvollständigen Liste soll die Sicherung der Verfügbarkeit und Überlebensfähigkeit von softwarebasierten Systemen durch Einsatz von zertifizierter und korrekter Software angesprochen werden.

Dazu gehört auch, dass weder eine nichtzertifizierte, noch nicht dokumentierte Software in sicherheitskritischen Systemen eingebunden werden sollte, um damit die Gefahr der Einschleppung von Trojanischen Pferden bzw. Viren zu bannen. Hier berühren sich die allgemeinen Qualitätsanforderungen mit den Forderungen an die Informationssicherheit. 8.4

Kurt Hechfellner, Dipl.-Ing.
Leiter der Abteilung
Technik Kommunikation, Siemens AG
Unterschleissheim