

Alarmübertragung und Internet

Widerspruch oder Realität ?

Durch den Preisverfall bei Internetzugängen und den, in der Bandbreite immer besser werdenden Backbone-Netzen, wird das öffentliche Internet für viele Kommunikationsmöglichkeiten immer attraktiver. Es liegt nahe, dieses Netz auch zur Meldungs- und Alarmübertragung zu nutzen. Bei Übertragung sicherheitsrelevanter und vertraulicher Informationen in öffentlichen Netzen sind jedoch Maßnahmen zum Schutz der Daten erforderlich.

Das Thema in Kürze:

Thema:

Alarmübertragung in öffentlichen Netzen

Problemstellung:

Sicherstellung von Manipulationssicherheit und Wegeüberwachung

Lösung:

Einsatz von Verschlüsselungs- und Authentifizierungstechnologien. Realisierung einer „End-to-End“ Verbindungsüberwachung.

Alarmübertragungssysteme höherer Sicherungsklassen erfordern, aufgrund von Richtlinien unterschiedlichster Institutionen, in der Regel zwei voneinander unabhängige Übertragungswege oder eine stehende Festverbindung. Bei stehenden Verbindungen muß eine Unterbrechung des Meldeweges in weniger als 20 Sekunden sowohl auf der Seite des Alarmübertragungsgerätes als auch an der Leitstelle angezeigt werden. Bisher werden für solche Verbindungen ausschließlich zu diesem Zweck geschaltete Standleitungen, das Datex-P-Netz der Telekom oder firmeneigene Datennetze mit geschlossener Benutzergruppe verwendet. Dieses bedeutet, daß Unberechtigte keinen Zugriff auf die Verbindungen haben. Die Kommunikation in diesen Netzen erfolgt isoliert, so daß im Bezug auf Datensicherheit keine besonderen Maßnahmen erforderlich sind. Der mit diesen Lösungen verbundene Nachteil sind die hohen laufenden Kosten.

Durch die Einführung verschiedener sehr preiswerter Zugangsmöglichkeiten zum

Internet, wie beispielsweise dem permanenten Zugang über B- oder D-Kanal des ISDN, wird die Nutzung öffentlicher Datennetze für firmeninterne Kommunikation zwischen verschiedenen Filialen eines Unternehmens immer attraktiver. Insbesondere durch die Einführung sogenannter Flatrates (Internetzugang zum Festpreis) lohnt sich die Nutzung öffentlicher Netze.

Es liegt somit nahe, das Internet auch zur Meldungs- und Alarmübertragung zu nutzen. Dieses setzt selbstverständlich die Anwendung von geeigneten Sicherheitsmechanismen voraus.

Da das Internetprotokoll selbst keine Sicherheitsvorkehrungen für eine geschützte Kommunikation vorsieht, müssen spätestens an den Übergangsstellen zu öffentlichen Netzen geeignete Maßnahmen ergriffen werden, damit vertrauliche Daten weder mitgelesen noch verändert werden können. Zusätzlich muß eindeutig sichergestellt werden, daß die Herkunft jeglicher, über das Internet übertragener Datenpakete, nachvollzogen werden kann.

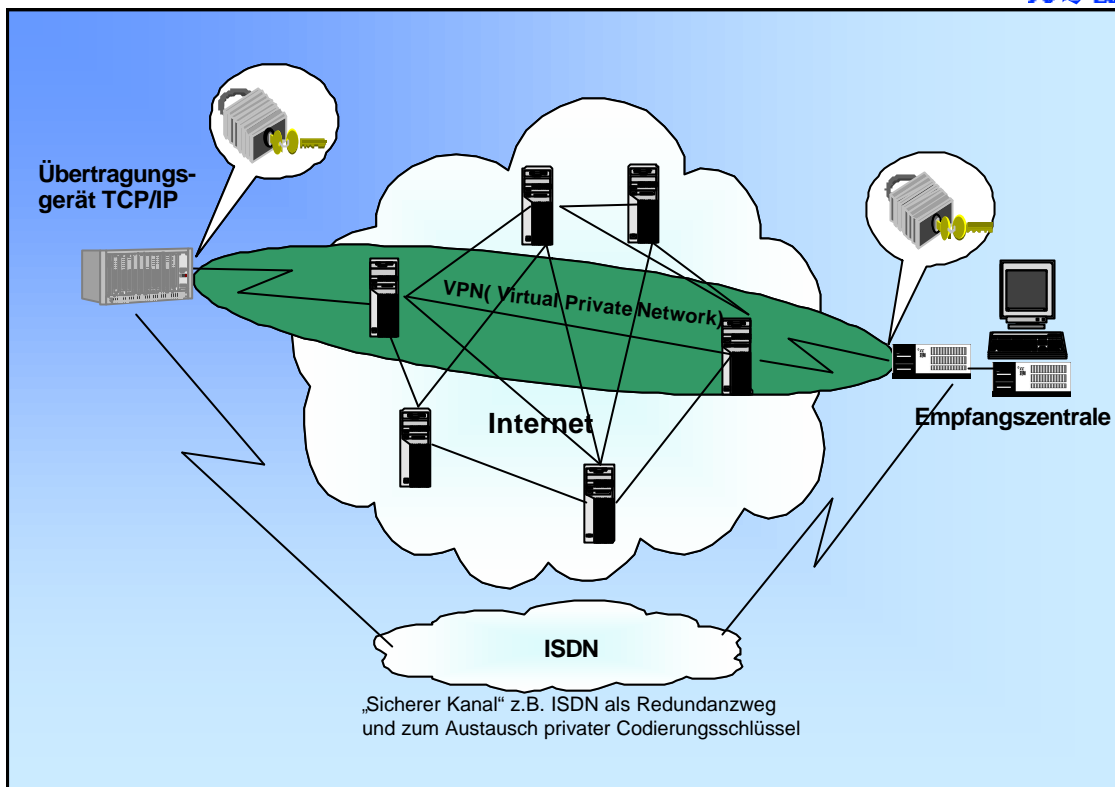


Abbildung 1: Bildung eines Virtual Private Network (VPN)

Um diese Forderungen zu erfüllen, bleibt nur die Möglichkeit, geeignete Codierungs- und Authentifizierungsverfahren anzuwenden. Durch die Anwendung dieser Verfahren ergibt sich dann ein sogenanntes Virtual Private Network (VPN).

Die Kommunikation im Bereich des öffentlichen Netzes erfolgt durch die Nutzung von VPN's abgeschottet von der Öffentlichkeit, da nur die Endanwendungen in der Lage sind die Datensätze zu decodieren. Der Begriff VPN bezeichnet dabei den Netzbereich, in dem die Kommunikation zwischen den festgelegten Nutzern Ende zu Ende, abgeschottet von der Öffentlichkeit, erfolgt.

Im Regelfall wird das IP-Protokoll um eine Verschlüsselungskomponente erweitert. Eine Lösung ist, das komplette herkömmliche IP-Paket zu verschlüsseln und es wiederum in ein anderes IP-Paket einzupacken (Tunneling). Für die gesicherte Übertragung ist jedoch nicht nur die eigentliche Verschlüsselung wichtig. Um verschlüsseln zu können, muß sowohl

die Methode, als auch mind. ein Schlüssel, auf beiden Seiten bekannt sein. Ansonsten kommen die Daten zwar gesichert an, können aber nicht auf der Gegenseite decodiert werden.

Der einzige Angriffspunkt auf die Sicherheit von VPN's ist im Allgemeinen die Vereinbarung und die Bekanntmachung von Schlüsseln bei den Kommunikationspartnern.

Ein möglicher, sicherer Weg ist, den Austausch der Schlüssel auf einen garantiert nicht angreifbaren Weg zu verlagern. In Frage kommt beispielsweise ein regelmäßiger Neuaustausch über Chipkarten oder über einen, komplett vom eigentlich zu schützenden Übertragungsweg getrennten Weg, wie z.B. dem öffentlichen Telefonnetz. Solche Verfahren haben sich in der Praxis bereits bewährt. Auch der Sicherheitsstandard „HBCI“, welcher von Kreditinstituten für das Onlinebanking über das Internet eingesetzt wird, baut auf diesen Verfahren auf. Den Herstellern entsprechender Übertragungstechniken bleibt es überlassen, auf bereits bestehende

Internetsicherheitsstandards zur Codierung und Authentifizierung aufzusetzen oder eigene Sicherheitslösungen mit den geforderten Eigenschaften zu entwickeln.

VPN's bieten damit den Effekt eines (virtuellen) kundeneigenen Daten-netzes, ohne teure Mietleitungen verwenden zu müssen. Ebenso entfällt die aufwendige Planung einer eigenen Netzstruktur. VPN's sind damit deutlich kostengünstiger und einfacher zu handhaben als Mietleitungen und andere virtuelle Festverbindungen, wie z.B. X31 im Datex-P Netz.

Dipl.-Ing. Stephan Holzem
Produktmanagement Security
Telefonbau A. Schwabe GmbH & Co. KG