Voice over IP aber sicher

Der Voice over IP Markt wächst stetig und es werden eine Vielzahl von Produkten und Dienstleistungen angeboten. Durch die Konsolidierung der Netze in diesem Bereich bieten sich völlig neue Möglichkeiten, die die konventionelle Telefonie dem Massenmarkt bisher nicht bieten konnte. Oft berücksichtigen Entscheider bei der Wahl von Voice over IP nur die potentielle Kostenersparnis und die flexible sowie einfache Verwendung. Dabei wird ein wesentlicher und neuer Aspekt vernachlässigt: die Sicherheit.

Grundsätzlich gelten für einen Netzwerkverkehr fünf Aspekte der Sicherheit: Verbindlichkeit, Vertraulichkeit, Verfügbarkeit, Authentizität und Integrität – sowohl für Voice over IP (VoIP) als auch für alle anderen vertrauenswürdigen Daten. Bei VoIP werden die Administratoren darüber hinaus mit völlig neuen Problemen konfrontiert, die in der herkömmlichen ISDN-Telefonie nie auftraten. Zunächst müssen die Datennetze, auf denen Sprache in Echtzeit

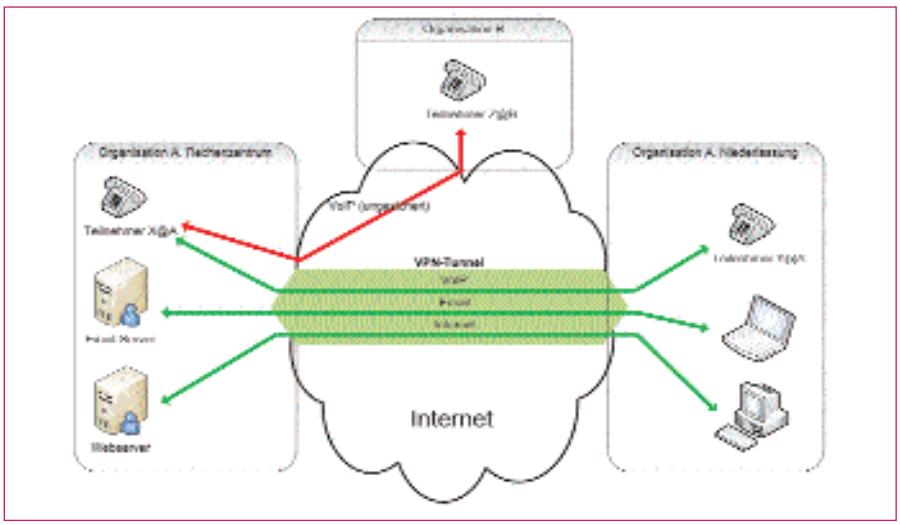

Abb.1: VoIP über eine VPN-Infrastruktur

übertragen wird, gewissen Qualitätsansprüchen bezüglich Paketverlustrate, „Ende-zu-Ende"-Verzögerung und Jitter (Abweichung der erwarteten Paketankunftszeit zur realen) genügen. Weiterhin rückt die Verfügbarkeit des VoIP-Dienstes in den Vordergrund, insbesondere auch in Hinblick auf die ständige Erreichbarkeit von Notruf-Diensten, aber auch die telefonische Erreichbarkeit.

Die Internettelefonie ermöglicht das Abhören von Gesprächen mit sehr einfachen Mitteln. War für das Belauschen von ISDN-Verbindungen zumindest spezielle – wenn auch nicht aufwendige – Hardware nötig, können VoIP-Verbindungen mit einem Standard-PC und frei erhältlicher Software abgehört werden. Sie sind damit vergleichbar unsicher wie E-Mails, die mit der Metapher einer für jeden lesbaren Postkarte stigmatisiert sind. Offene Sicherheitsstandards bieten verschiedene Ansätze, die Sprachkommunikation über Datennetze abzusichern, und stellen die Grundlage für eine organisationsübergreifende Telefonabsicherung dar. Um diese Sicherheitsstandards anzuwenden, müssen zunächst die Charakteristika von VoIP-Daten betrachtet werden.

Es gibt bei VoIP zwei unterschiedliche Arten von Daten: die Signalisierung und die eigentlichen Telefongesprächsdaten (Medienstrom). Die Signalisierung ist die Anrufsteuerung und unter anderem verantwortlich für den Anrufauf- und -abbau, die Anrufweiterleitung sowie die Konferenzsteuerung. Des Weiteren handelt sie auch die Parameter einer Telefonverbindung aus, wie z.B. das Festlegen des zu verwendenden Sprach-Codecs und den UDP-Port der Sprachkanäle. Der populärste Vertreter der Signalisierungsprotokolle ist das Session Initiation Protocol (SIP). Für die Übertragung der Sprachdaten wird das Real-Time Transport Protocol (RTP) verwendet, das unter anderem die Sendereihenfolge von Paketen markiert und Isochronität garantiert.

Sicherheit der Kommunikation

Bei der Verwendung von VoIP spielen besonders die Sicherheitsdienste Verschlüsselung und Authentisierung von Daten eine wichtige Rolle. Die eigentlichen Gespräche können „Ende-zu-Ende" verschlüsselt werden, die Signalisierung dagegen enthält meistens Informationen für die Intermediäre (VoIP-Server, Firewalls usw.) und muss dort folglich in unverschlüsseltem Zustand vorliegen. Aus diesem Grund ist nur eine „Hop-zu-Hop"-Verschlüsselung der Signalisierung sinnvoll.
Grundsätzlich wird zwischen zwei Arten von Sicherungsmechanismen unterschieden: die VoIP-spezifischen Standards und die „allgemeinen Sicherheitsstandards".

Zu den **allgemeinen Sicherungsmaßnahmen** zählen VPN-Lösungen (Virtual Private Network). VPNs haben den Vorteil, transparent sämtlichen Netzwerkverkehr zwischen zwei oder mehreren Netzen abzusichern, ohne dass VoIP-spezifische Anpassungen vorgenommen werden müssen. Da der Verschlüsselungskanal (Security Association, SA) bei einem VPN meistens unabhängig von dessen Bedarf permanent besteht, ist es nötig, dass die verwendeten Schlüssel regelmäßig aktualisiert und ausgetauscht werden. Analysen und Messungen am Institut für Internet Sicherheit haben ergeben, dass dieses Re-Keying während eines Gesprächs durchaus Einfluss auf die Qualität der Verbindung und damit auf die Qualität des Telefongespräches haben kann, wenn der Neuaufbau einer SA zeitgleich mit dem Ablaufen der alten SA geschieht. Um dieses Problem zu vermeiden, muss die VPN-Lösung in der Lage sein, neue SAs rechtzeitig vor dem Ablaufen der momentan verwendeten SA zu erzeugen. Darüber hinaus hat eine generische Lösung wie ein VPN jedoch den Nachteil, dass die Sicherung erst an der Grenze des lokalen Netzes beginnt bzw. endet. Im LAN werden alle Sprachdaten unverschlüsselt übertragen

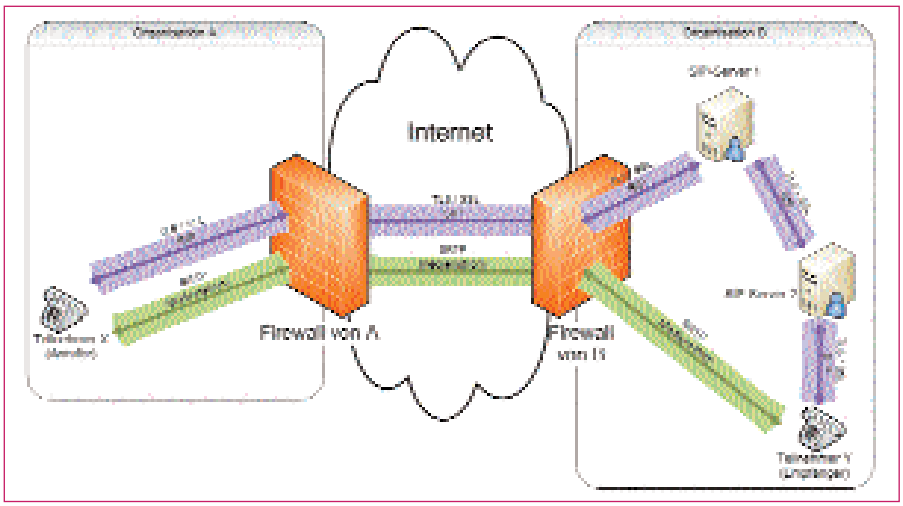

Abb.2: SIP wird „Hop-zu-Hop" via TLS verschlüsselt, der Medienstrom „Ende-zu-Ende" via SRTP

und können dort einfach im Klartext abgegriffen werden. Außerdem sind VPN-Vernetzungen – und damit die Kopplung von unterschiedlichen Firmennetzen - organisationsübergreifend aufwendig zu organisieren, weshalb eine flächendeckende VoIP-Absicherung oft scheitert. Für den organisationsinternen VoIP-Verkehr stellen VPNs allerdings eine einfache Möglichkeit dar.

Anders als VPNs stellen **VoIP-spezifische Sicherheitsstandards** Funktionen oder Erweiterungen zu den VoIP-Protokollen SIP, H.323, IAX2 und RTP dar.
Da bevorzugt SIP in Kombination mit RTP eingesetzt wird, ist die gängigste Lösung, SIP via TLS gesichert „Hop-zu-Hop" zu übertragen und den Medienstrom nach dem SRTP-Standard (Secure RTP) „Ende-zu-Ende" zu sichern (siehe Abb. 2). Von entscheidender Bedeutung ist hierbei die Vertrauenskette zwischen den an der Signalisierung beteiligten Intermediären. Die für SRTP benötigten Schlüssel werden in den Signalisierungsnachrichten (SIP) ausgetauscht. Wird das ausgetauschte Schlüsselmaterial nicht ausschließlich über vertrauenswürdige Intermediäre zu den Gesprächsteilnehmern geleitet, besteht die Gefahr von „Man-In-The-Middle-Angriffen", welche die Gesprächssicherheit kompromittieren.
Des Weiteren ist eine organisationsübergreifende Public Key Infrastruktur (PKI) Voraussetzung, um Kommunikationspartner zu authentifizieren. Eine entsprechende PKI ist z.B. auch Voraussetzung für eine gesicherte E-Mail-Kommunikation. In Anbetracht der Tatsache, dass sich eine weitflächige PKI für den E-Mail-Dienst nicht durchsetzten konnte, bleibt auch zweifelhaft, ob sich verbreitetes sicheres Telefonieren mit den etablierten VoIP-Standards durchsetzten wird.
Wie einfach eine flächendeckende Verschlüsselung erreicht werden kann, zeigt der Erfolg von SSL bei Webseiten (HTTPS). Durch in Browsern vorinstallierte Root-Zertifikate ist die gesicherte Benutzung von Webseiten „out-of-the-box" möglich, was ein entscheidender Vorteil ist. Allerdings erkaufen sich die Betreiber gesicherter Webseiten den Schutz bei Trustcentern für Beträge, die nur die wenigsten Organisationen bereit sind zu zahlen. Dieser Nachteil ließe sich nach diesem Modell auch bei VoIP nicht vermeiden.
Schließlich ist ein grundsätzliches Problem aller vorgestellten Sicherheitsmaßnahmen der entstehende Overhead der Daten, die bei verschlüsselten Sprachdaten mit übertragen werden müssen. In Anbetracht der Tatsache, dass Sprachpakete sehr klein und der Verschlüsselungs-Overhead konstant pro Paket ist, entsteht ein Mehr an Daten von deutlich über 25 Prozent, abhängig von Verschlüsselungsmodus und Sprach-Codec. Dieser Overhead kann durch transparente Kompression zum Teil ausgeglichen werden, was jedoch auf leistungsschwachen Rechnern die Verbindungsqualität beeinflussen kann. Die meisten modernen Systeme bewältigen allerdings Verschlüsselung, Authentisierung und Kompression von VoIP Daten in qualitativ guten Netzen problemlos.

Ausblick

Mit der Sicherheit (Verschlüsselung und Authentikation) ist allerdings nur eines der Probleme, die mit der fortschreitenden Verwendung von VoIP entstanden sind, behandelt. Darüber hinaus werden durch den paketvermittelten Charakter besondere Echtzeitanforderungen an die Datennetze gestellt. Eine Tatsache, über die man sich in den leitungsvermittelten Telefonnetzen keine Gedanken machen musste. Diese Qualitätsanforderungen (Quality of Service - QoS) und wie sich die in diesem Artikel beschriebenen Sicherungsmaßnahmen in qualitativ unterschiedlichen Netzen darauf auswirken, sind Thema eines Folgeartikels in einer der nächsten Ausgaben.

Peter Backs forscht im Rahmen seiner Diplomarbeit im Bereich „Sicherheit von Voice over IP" im Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen.

Prof. Dr. Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssi-cherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de).

DATAKONTEXT TAGUNGEN

Datenschutz Kompakt
18.-19.09.2007 in Köln

Repetitorium GDDcert.
25.09.2007 in Berlin

Besondere Anforderungen beim Datentransfer ins Ausland
26.09.2007 in Köln

Rechtssichere Personaldatenverarbeitung und Prozess
27.09.2007 in Berlin

Datenschutz Teil 1 - Einführung in den Datenschutz für die Privatwirtschaft
08.-12.10.2007 in Bad Neuenahr

Datenschutz Aktuell
16.10.2007 in Berlin

Der neue Telemediendatenschutz bei Internet und E-Mail
18.10.2007 in Frankfurt/M.

weitere Informationen unter:
DATAKONTEXT-TAGUNGEN GmbH & Co. KG
Postfach 4128 · 50217 Frechen
Tel 02234/65633 oder 65638 · Fax 65635
tagungen@datakontext.com