Gefahren drohen auch aus dem eigenen lokalen Netzwerk:

Auerswald Whitepaper: VoIP-Security

Mit Voice-over-IP sicher telefonieren

Dank wachsender Bandbreiten und moderner Quality-of-Service-Mechanismen hat die IP-Telefonie ihre Kinderkrankheiten inzwischen erfolgreich hinter sich gelassen. Gute Sprachqualität, umfangreiche Komfortfunktionen und nachhaltige Kosteneinsparungen machen den Einsatz von VoIP-Lösungen für Unternehmen heute zunehmend attraktiv. Doch wie steht es um die Sicherheit der IP-basierten Sprachübertragung? Umfassenden Schutz bieten hier vor allem professionelle ITK-Systeme spezialisierter Hersteller.

97286_03 04/2016

Auerswald GmbH & Co. KG, 38162 Cremlingen-Schandelah,
Infoline: +49(0) 53 06/92 00–700, www.auerswald.de

Auerswald®
Clever Communications

Auerswald Whitepaper: VoIP-Security

Das Telefonsystem gehört zu den zentralen Infrastruktureinrichtungen eines Unternehmens und ist somit besonders schützenswert. Längere Ausfallzeiten sind in der modernen Kommunikation ebenso wenig tolerabel wie die Kompromittierung von Verbindungsdaten oder gar Gesprächsinhalten. Dies gilt auch für die Sprachübertragung mit Voice-over-IP, auf die vor allem immer mehr kleine und mittelständische Unternehmen aus Gründen der Kostenreduzierung umrüsten. Denn von den anfänglichen Hindernissen der Internettelefonie ist mittlerweile kaum noch was zu spüren; die nervigen Aussetzer, Echos, Gesprächsabbrüche oder Erreichbarkeitsprobleme sind weitgehend vom Tisch. Heute dominieren die Vorteile der VoIP-Technik: Die einfachere Administration, eine unkompliziertere Infrastruktur und die Integration in andere Dienste und Prozesse lassen Industrie und Gewerbe zunehmend umdenken – und bieten damit ITK-Beratungsunternehmen, Systemhäusern und dem ITK-Fachhandel ein lukratives Markt- und Absatzpotenzial.

Gefahren für das einheitliche Netzwerk

Doch mit zunehmender Verbreitung der Internettelefonie steigen auch die Gefahren und Sicherheitslücken, die durch VoIP-Telefonate entstehen können. Denn während die klassische Telefonie auf einer geschlossenen Punkt-zu-Punkt-Verbindung beruht und deshalb schon allein aus struktureller Sicht ein hohes Maß an Sicherheit bietet, nutzt VoIP zur Übertragung das offene IP-Netz: Hier verschmelzen Daten- und Sprachkommunikation in einem gemeinsamen Netzwerk. Anders als im herkömmlichen Festnetz werden die Daten beim VoIP-Verfahren in einzelne Pakete zerlegt, separat übertragen und auf der Empfangsseite wieder zusammengesetzt. So gelangen VoIP-Gespräche in einem gemeinsamen Datenstrom mit E-Mails, Webseiten und anderen Dateien zum Empfänger. Dabei verbessern Quality-of-Service-Lösungen zusätzlich die Qualität beim Telefonieren, da Verzögerungen oder Datenverluste bei der Übertragung die Sprachqualität erheblich beeinträchtigen können. All das schafft einerseits mehr Flexibilität, öffnet jedoch auch potenzielle Schwachstellen, wenn keine zusätzlichen Sicherungsmaßnahmen für die Übertragung der Sprachdaten ergriffen werden.

Denn leider spiegelt sich das Sicherheitsbedürfnis zeitgemäßer Kommunikation nicht in der Art der verwendeten VoIP-Übertragungsprotokolle wieder. Selbst das heute am weitesten verbreitete SIP Protokoll (Session Initiation Protocol) sieht weder zwingend eine sichere Authentifizierungsmethode vor, noch eine Verschlüsselung der Gesprächsdaten. Dabei bilden Protokolle wie SIP die Basis für sämtliche Unified-Communication-Lösungen und gelten damit als wichtige Grundlage für die Bereitstellung von IP-Sprachdiensten innerhalb moderner Office- und Collaboration-Anwendungen. Werden also VoIP- Verbindungen über SIP ohne zusätzliche Sicherheitsvorkehrungen aufgebaut und die Protokollinformationen unverschlüsselt übermittelt, können diese von potenziellen Angreifern komplett eingesehen werden.

Verschiedene Angriffsszenarien

Dieser Umstand öffnet Attacken wie dem Abhören und Mitschneiden von Telefonaten, Identitätsdiebstahl, Gebührenbetrug oder gar nachträglichen Manipulationen von Gesprächen Tür und Tor. Selbst die komplette Übernahme eines ITK-Systems ist für einen Angreifer ohne weiteres möglich, wenn er sich über ungesicherte IP-Zugänge oder eine Portfreischaltung im Router den Zutritt zum ITK-System verschaffen kann. Über eine Rufumleitung auf sein eigenes System lassen sich so beispielsweise Anrufe von speziellen Servicerufnummern wie 0137 oder 0900 über die feindlich übernommene Anlage zum eigenen Vorteil nutzen. Richtet sich der Angreifer über das Internet gar als Nebenstelle der gekaperten ITK-Anlage ein, verfügt er zudem über kostenlose Einwahlzugänge in das Fest- und Mobilnetz. Dann erleben Unternehmen bei der Telefonabrechnung mitunter böse Überraschungen, wie jüngst ein Betrieb im rheinland-pfälzischen Grünstadt: Hacker hatten sich unbemerkt Zugriff in das Telefonnetz verschafft und einen Schaden von 11.000 Euro verursacht. Zu Zeiten, als kein Mitarbeiter mehr im Haus war, führten die Täter über das Firmen-Telefonnetz teure Gespräche ins Ausland. Weitaus gefährlicher sind jedoch Angriffe, die Nachrichten auf dem Netzwerk manipulieren oder gänzlich neue Nachrichten an das Opfersystem versenden. Eine bekannte Attacke nennt sich „Man-In-The-Middle“. Hierbei schaltet sich der Angreifer zwischen die Kommunikationspartner und erlangt Kontrolle über den Datenverkehr. Dabei täuscht er die Gesprächsteilnehmer, indem er ihnen jeweils die Identität (IP- und MAC-Adresse) des anderen vorspiegelt. Auf diese Weise lassen sich ausgetauschte Nachrichten beliebig verfälschen oder eigene Nachrichten in fremdem Namen senden.

Kollege hört mit

Damit wird auch deutlich: Für die verlässliche Einführung von VoIP ist es mit dem einfachen Anschließen eines VoIP-Servers und von IP-Telefonen an ein bestehendes Datennetzwerk nicht getan. Denn Gefahr droht nicht nur aus der weiten Ferne des Webs, sondern vor allem aus den eigenen Reihen, wie dies Studien seit Jahren belegen. Gründe dafür gibt es viele – sei es, dass Mitarbeiter planen, dem Unternehmen gezielt Schaden zuzufügen, oder sich durch die Erschleichung von sensiblen Informationen persönliche Vorteile versprechen. Für solche Ansinnen geben mangelhaft gesicherte VoIP-Systeme ein nahezu perfektes Ziel ab. Denn vielen Nutzern ist gar nicht klar, dass sie gerade über eine IP-Verbindung telefonieren, so dass im guten Glauben vermeintlicher Festnetzsicherheit beliebige vertrauliche Inhalte ausgetauscht werden. Besonders brisant sind dabei Telefonate der Geschäftsleitung, des Personalwesens oder der Entwicklungsabteilung.

Wie einfach solche VoIP-Gespräche im Prinzip abzuhören sind, zeigen weit verbreitete und simpel zu bedienende Sniffer-Programme, die sich heute jederzeit legal als Open-Source-Software aus dem Internet herunterladen lassen. Sogar spezielle Voreinstellungen für die Filterung von VoIP-Telefonaten sind in den Tools bereits enthalten. Eine Analyse liefert umfangreiche Informationen über die Identität der Gesprächsteilnehmer, Zeitpunkt und Dauer der Telefonate und den jeweiligen Gesprächsstatus. Der Zugriff auf fremde Voicemail-Boxen ist dabei ebenso möglich wie das Abhören und Überwachen der Endgeräte mit Mikrofon oder Kamera. Der Clou: Um ein per Sniffer mitgeschnittenes Gespräch abzuspielen, genügt ein einfacher Mausklick. Die Software ordnet die Audiodaten des Gespräches sogar automatisch den jeweiligen Authentifizierungsinformationen, welche die Nutzeridentität enthalten, zu.

Verschlüsselung ist Pflicht

Um derartige Angriffe zu unterbinden, ist eine Verschlüsselung der VoIP-Kommunikation unerlässlich. Höchstmöglichen Schutz bietet hier die Kombination aus SIPS (Session Initiation Protocol Secure) und SRTP (Secure Real Time Transport Protocol). SIPS sorgt als sichere Variante des SIP-Protokolls für einen verschlüsselten Verbindungsaufbau und schützt so Server (Telefonanlage) und Client (IP-Telefon) zuverlässig gegen feindliche Zugriffe. Die Sprachdaten selbst müssen jedoch zusätzlich mit SRTP abgesichert werden. SRTP kodiert die Sprachdaten mit einem 128-Bit AES-Schlüssel (Advanced Encryption Standard), teilt diese in Datenpakete auf und versendet sie über das Netzwerk. Um durchgängige Sicherheit zu gewährleisten, ist es zwingend erforderlich, dass sowohl die Telefonanlage als auch alle verwendeten IP-Telefone für die benötigte Ver- und Entschlüsselung ausgelegt sind. Solche VoIP-Telefonsysteme mit integrierter Verschlüsselung werden von Spezialisten wie etwa Auerswald angeboten und garantieren Sicherheit auf höchstem Niveau.

Unterschiedliche Anforderungen an die Sicherheit

Denn wie hoch der Aufwand zur Absicherung der IP-Telefonie ist, hängt nicht zuletzt von der verwendeten VoIP-Lösung ab. Entscheidet sich ein Unternehmen dazu, VoIP einzuführen, stehen im Wesentlichen zwei verschiedene Lösungen zur Wahl: Soft-PBX oder Hard-PBX, zu denen auch ISDN-Telefonanlagen mit integrierter VoIP-Funktionalität zählen, sogenannte Hybrid-Telefonanlagen.

Basis von Soft-PBX-Lösungen ist eine Telefonsoftware, die auf einem herkömmlichen Rechner mit Linux- oder Windows-Betriebssystem installiert wird. Solche Systeme sind meist sehr preisgünstig in der Anschaffung, setzen aber voraus, dass die mitunter komplexe Wartung der Software auch verlässlich von der firmeneigenen EDV geleistet werden kann. Denn ansonsten drohen hohe Kosten für externe Dienstleister, sobald Updates anstehen oder Wartungsarbeiten durchgeführt werden müssen.

Für Unternehmen ohne spezialisierte IT-Mannschaft stellt die Hardware-PBX beziehungsweise eine Hybrid-Anlage die perfekte Einstiegslösung dar. Sie ist vergleichbar mit einer herkömmlichen ISDN-Telefonanlage, die sowohl alle klassischen Funktionen einer TK-Anlage als auch moderne IP-Telefonie beinhaltet. Solche Anlagen von spezialisierten Herstellern wie Auerswald sind enorm zuverlässig und weisen eine sehr gute Sprachqualität auf. Im Gegensatz zu Soft-PBX-Lösungen bieten sie ein in sich geschlossenes und geschütztes System, bestehend aus hochwertiger Hardware und einem gehärteten Betriebssystem. Sicherheits- und Funktions-Updates werden dabei direkt vom Hersteller

Auerswald Whitepaper: VoIP-Security

bereitgestellt und lassen sich auch von Nicht-Spezialisten schnell und einfach installieren. Ein weiterer Vorteil von Hybrid-Systemen ist, dass ISDN- und IP-Telefonie gemeinsam genutzt werden können. Dadurch ist eine sanfte Migration ohne abrupte Umstellung möglich. So kann etwa schrittweise auf IP-Telefonie umgestiegen werden, ohne dass es zu Unterbrechungen im Tagesgeschäft kommt.

Dank Verschlüsselung so sicher wie klassische Telefonie

Werden die richtigen sicherheitstechnischen und organisatorischen Maßnahmen getroffen, ist die IP-Telefonie für Unternehmen genauso sicher wie die klassische Telefonie. Sicherheitsmaßnahmen verteilen sich dabei auf mehreren Ebenen.

Während IP-Telefonie-Server durch den Einsatz speziell optimierter Betriebssysteme sowie Firewalls und Viren-Scanner geschützt werden müssen, ist für die Sicherheit der Kommunikation vor allem die Verschlüsselung mittels SIPS und SRTP obligatorisch. Mit der COMpact 4000/5000/5000R bzw. der COMmander-Serie bietet Auerswald jeweils ein hybrides VoIP-System, das selbst den höchsten Sicherheitsstandards genügt. Zusammen mit den COMfortel IP-Systemtelefonen ist ein flächendeckender Einsatz verschlüsselter Kommunikation mittels SIPS und SRTP gerade für mittelständische Unternehmen leicht umzusetzen. Selbst für den Fall, dass Mitarbeiter grundlegende Sicherheitsregeln missachten, bieten IP-Systemtelefone von Auerswald (ab COMfortel 1400 IP aufwärts) zusätzlich eine „Fingerprint"-Funktion, die einen Missbrauch durch nicht autorisierte Nebenstellen wirkungsvoll verhindert.

Weitere Ideen zu maßgeschneiderten Lösungen finden Sie auf www.auerswald.de