VoIP? Aber sicher doch!

Voice over IP (VoIP) ist die Übertragung von Sprache über das Internet und steht immer mehr im Fokus des Interesses von Anwendern: Die Frage, wie angreifbar die IP-Telefonie ist, gewinnt daher ebenfalls an Bedeutung. FACTS hat zu diesem Thema den Entwicklungsleiter bei Agfeo Ralf Weinbrecher befragt.

FACTS: *Wie beurteilen Sie die Entwicklung von Voice over IP (VoIP) in den vergangenen Jahren?*

Ralf Weinbrecher: Die Akzeptanz von VoIP hat inzwischen aufgrund der steigenden Verbreitung von Breitband-Internetanschlüssen, aber auch wegen der technologischen Weiterentwicklungen bei unseren Kunden stark zugenommen. Ein weiterer Grund für das große Interesse an VoIP ist die Ankündigung der Deutschen Telekom, bis zum Jahr 2018 sämtliche ISDN-Anschlüsse in Deutschland in All-IP-Anschlüsse umzuwandeln.

FACTS: *Welche Gefahren sehen Sie?*

Weinbrecher: Mit steigender Verbreitung der VoIP-Technologie wächst natürlich auch das Bedrohungspotenzial. IT-Administratoren und Errichter von VoIP-TK-Systemen müssen daher möglichst viele Angriffsszenarien kennen, um den Anwender vor Schaden zu schützen. Grundsätzlich gelten für die Absicherung von VoIP-Systemen gegen Eindringlinge die gleichen Regeln, wie man sie allgemein bei sicherer Netzwerk-Kommunikation im Unternehmen anwendet.

FACTS: *Wie sieht der Schutz vor Angriffen genau aus?*

Weinbrecher: Die Aufgabe des IT-Administrators ist es, im Unternehmensnetzwerk nur authentisierten Geräten und Benutzern den Zugang zu erlauben. Zur Sicherung des Zugangs und der Authentifizierung der Benutzer sollten Sicherheitszertifikate eingesetzt werden. Erfolgt die Benutzer-Authentifizierung nur mittels Benutzername und Passwort, so sind unbedingt als sicher eingestufte Passwörter einzusetzen. Die Verschlüsselung der Sprachpakete sowie der Signalisierungsebene ist ebenfalls unbedingt erforderlich. Unverständlich ist, dass derzeit kaum einer der bekannten und flächendeckend auftretenden SIP-Provider (SIP = Session Initiation Protocol) eine Verschlüsselung unterstützt.

Im Normalfall läuft die VoIP-Kommunikation außerhalb des eigenen Netzwerks unverschlüsselt ab.

FACTS: *Was würden Sie zum Schutz von VoIP-Ressourcen empfehlen?*
Weinbrecher: Zum Schutz der VoIP-Ressourcen im Unternehmen empfiehlt sich der Einsatz getrennter VLANs für Sprache und Daten. Der VoIP-Verkehr sollte auf möglichst wenige VLANs begrenzt werden. Durch die Trennung von Sprache und Daten lässt sich die VoIP-Infrastruktur auch effektiver gegen Angriffe schützen und der Sprachverkehr besser priorisieren.

FACTS: *Wie lässt sich der Schutz außerhalb der VLANs realisieren?*
Weinbrecher: Außerhalb der VLANs können spezielle Firewalls, die nur bestimmte Protokolle zulassen und nur autorisierten Benutzern den Zugang öffnen, schützen. Dadurch wird auch gewährleistet, dass die VoIP-Ressourcen, also beispielsweise die TK-Anlage, nicht direkt dem Zugriff aus dem Internet ausgesetzt ist. Um die TK-Anlage auch aus der Ferne zu warten, sollte unbedingt das Agfeo-Fernwartungssystem angewendet werden.

FACTS: *Was würden Sie dem IT-Administrator in Bezug auf die Sicherheit von VoIP-Systemen raten?*
Weinbrecher: Die IT-Administratoren tragen die Verantwortung für den Einsatz effektiver Monitoring-Werkzeuge, die es gestatten, Angriffe und Unregelmäßigkeiten im VoIP-Netz schnell zu entdecken und zu analysieren. Wichtig ist natürlich auch die regelmäßige Wartung der Systeme durch Updates. Das betrifft alle Komponenten des Systems, angefangen bei den Endgeräten bis zur TK-Anlage. Die Koppelung von Standorten oder die Anbindung externer Nebenstellen sollte immer über sichere VPN-Tunnel erfolgen.

„Wir als Hersteller führen regelmäßige Sicherheits-Überprüfungen der Komponenten unserer Firmware durch und bieten für unsere Software regelmäßig Updates und Patches an.“

RALF WEINBRECHER,
Entwicklungsleiter bei Agfeo

FACTS: *Was trägt Agfeo als Hersteller nachhaltig zur Sicherheit bei?*
Weinbrecher: Wir als Hersteller führen regelmäßige Sicherheitsüberprüfungen der Komponenten unserer Firmware durch und bieten für unsere Software regelmäßig Updates und Patches an, denn die Sicherheit von VoIP-Netzwerken hängt von den zugrunde liegenden Betriebssystemen und den jeweiligen Anwendungen ab. Daher ist es zwingend notwendig, die Betriebssysteme und die VoIP-Anwendungen regelmäßig zu pflegen und die Installation der neuesten Patches vorzunehmen.

FACTS: *Welches Fazit würden Sie ziehen?*
Weinbrecher: Bei der Installation und Wartung von VoIP-Infrastrukturen gilt es, diverse Sicherheitsregeln zu beachten. Der Eindruck, dass VoIP-Technologie grundsätzlich unsicherer ist als die klassische ISDN-Technik, ist jedoch falsch. Die sichere Einrichtung einer VoIP-Infrastruktur setzt Kenntnisse auf dem IT-Sektor voraus. Wir als Hersteller von Hybrid-TK-Anlagen bieten mit unseren Produkten in sich abgeschlossene Systeme an. Diese Produkte basieren auf zuverlässiger, energiesparender und leistungsfähiger Hardware. Zum Einsatz kommen spezialisierte, speziell auf die Anwendung zugeschnittene Softwarepakete. Eine Aufgabe unserer Entwicklungs- und Qualitätssicherungs-Abteilungen besteht darin, das Betriebssystem und die Anwendungen dieser Hybrid-TK-Systeme gegen Bedrohungen jeder Art zu schützen. Unsere regelmäßigen Sicherheits- und Service-Updates lassen sich einfach installieren. Die Ausstattung unserer Produkte mit klassischen ISDN-Schnittstellen sowie mit VoIP-Technologie erlaubt den Kunden zudem den sanften Übergang zur IP-Kommunikation.

Klaus Leifeld ■