Auf Nummer sicher

Voice over IP erobert unaufhaltsam die Büros. Mit all den Vorteilen kommen auch Vorbehalte, vor allem in puncto Sicherheit. Eins ist klar: VoIP bringt grundsätzlich keine Gefahren, die es nicht schon ohnehin durch Internet, Email oder eigene Mitarbeiter gibt. Mittlerweile ist die Technologie so weit gereift, dass sie auch Unternehmen genug Möglichkeiten bietet, sich erfolgreich gegen Eindringlinge zu wehren und VoIP-Installationen abzusichern.

Der große Vorteil der Internettelefonie für Unternehmen liegt auf der Hand: Die Konvergenz von IT- und TK-Infrastruktur ermöglicht die Anbindung anderer nützlicher Applikationen wie Email und Datenserver im LAN. Einerseits lassen sich so jede Menge Kosten einsparen, die neuen Applikationen vereinfachen zudem erheblich den Arbeitsalltag. Andererseits werden die Bedrohungen der IT-Infrastruktur auch zur Bedrohung des VoIP-Systems. Schlimmer noch: das Telefonsystem kann nun aufgrund des gemeinsamen LAN von den Arbeitsplätzen innerhalb des Unternehmens attackiert werden.

Welche Gefahren lauern

In der heutigen Konvergenzwelt gilt es zwei Sicherheitsproblemen vorzubeugen. Das erste ist die Abhörsicherheit. Benötigt man zum Abhören von Gesprächen der herkömmlichen Telefonie noch physischen Zugang zum Kabel, eröffnet die Internettelefonie Hackern ganz neue Spielarten für illegale Aktivitäten. Mit aktuellen Hackerprogrammen wie Cain & Abel und einem PC im LAN lassen sich Telefongespräche aufzeichnen, in WAV-Files umwandeln und so für eine spätere Nutzung konservieren. Der Zugang zum ungeschützen LAN ist alles was man braucht, und den bekommt man vom unternehmensinternen PC leicht.

Das zweite große Problem sind die DoS-Attacken (Denial of Service), begünstigt durch jede Menge unsicheres und instabiles VoIP-Equipment am Markt. Oft findet man noch VoIP-Geräte im Einsatz, die in Sachen Sicherheit und Funktionalität mit Features ausgestattet sind, die bei weitem nicht den neuesten Standards entsprechen. Netzwerkmanipulation ist dort um ein Vielfaches leichter, und für einigermaßen Versierte lässt sich im Handumdrehen das Gerät außer Gefecht setzen.

Ein Albtraum für alle Anwender: Permanentes Klingeln, immer wieder Rebooten der Telefone oder andere Ärgernisse wie unerwünschte Nachrichten auf dem Display können passieren, wenn man an Sicherheitsvorkehrungen der kompletten IT-Struktur wie auch des VoIP-Systems gespart hat. Ein Shell Script zu schreiben - dafür braucht es lediglich ein paar Programmierzeilen. PC-Nutzer, die etwas mehr Zeit verwenden, lesen die jüngsten Bugs in ihrer IP-PBX, um diese mit einem „Invite to Death“-Paket so richtig crashen zu lassen (siehe z.B. www.voipsa.org). Da für Hacker VoIP zunehmend interessanter wird, sind künftig auch Viren denkbar, die einen Code enthalten, der das Mithören ermöglicht oder gleich den PBX Server in die Knie zwingt.

Mittlerweile gibt es Anbieter am Markt, die VoIP-Alarmsysteme anbieten (z.B. www.sipera.com). So wie es Sicherheitsanlagen gibt, die unerlaubtes Betreten von Büroräumen melden, so beobachten VoIP-Alarmsysteme das Netzwerk und senden Alarmsignale an den IT-Administrator, wenn sich ein ungewollter Eindringling zu schaffen macht. Doch das sollte nicht der einzige Schutz sein.

VoIP braucht sichere Infrastruktur

Manchmal ist es lediglich ein schlechtes Netzwerk-Setup, das DoS-Probleme auslöst. Wenn man beispielsweise Sprach-Paketen zwischen dem Büro und dem Service-Provider keine Priorität einräumt, sollte man nicht allzu überrascht sein, wenn ein einfacher Email-Download-Zugang zur unbeabsichtigten DoS-Attacke von laufenden Telefonaten wird. In diesem Fall verdrängen die ankommenden Email-Pakete sämtliche verfügbare Bandbreite und die Audio-Datenpakete schaffen es nicht mehr rechtzeitig zum Empfänger.

Um sicher zu gehen, dass wenigstens das LAN den Voice-Daten höhere Priorität verschafft, sollte man auf Virtual Local Area Network (VLAN) setzen. Fast alle modernen Switches unterstützen VLAN-Tagging, das dem Switch signalisiert, zu welchen VLAN das zu verarbeitende Ethernetpaket gehört. Das löst auch schon den größten Teil des Problems. Wenn darüber hinaus der Ethernet Switch auch Bandbreitenlimitierung auf Trunks unterstützt, können ankommende Attacken abgewehrt werden, bevor sie das Gerät erreichen.

Bezüglich Firewalls ist immer wieder zu hören, dass diese alle ein- und ausgehenden Daten verstehen müssten, das heißt auch SIP-Daten. Bei älteren Firewalls können durchaus Probleme in Sachen VoIP und SIP auftreten. Moderne Firewalls erkennen jedoch zunehmend VoIP- und SIP-Datenpakete und sichern deren ungestörtes Durchkommen, indem sie den Paketen die entsprechende Priorität geben. Einige Firewalls übernehmen sogar das Verschlüsseln von unverschlüsselten SIP- und RTP-Daten und übersetzen diese in sichere TLS- und SRTP-Pakete (z.B. InGate oder Borderware).

Bei der Installation eines kostenfreien Softphones auf dem PC ist gehörig Vertrauen in die Ehrlichkeit des Herstellers gefordert. Nutzt eine Applikation ein eigenes, verschlüsseltes Protokoll für die Kommunikation nach draußen, kann die Firewall nicht mehr beurteilen, ob gerade telefoniert wird oder Unternehmensdaten auf den Rechner eines Angreifers hochgeladen werden. Kann der Hersteller eines solchen Softphones der kleinen Hintertür in der Software widerstehen? Im Gegensatz zu anderer Software braucht das Softphone legitim die Verbindung durch die Firewall, so dass Benutzer und Administrator entsprechende Sicherheitshinweise ignorieren und die Software gewähren lassen. Der klassische Fall eines Trojanischen Pferdes: Eine nett verpackte Angriffswaffe in Form eines Geschenks.

Während SBC (Session Border Controller) für Internet Service Provider zum Standard gehören, erkennen inzwischen auch Unternehmen deren Nützlichkeit für den reibungslosen VoIP-Telefonbetrieb. Der so genannte Mini-SBC regelt beispielsweise den Sprachdatenfluss in beide Richtungen und gewährleistet, dass das Markieren von Paketen sauber funktioniert.

VPN ist sinnvoll für die Lösung der meisten Sicherheitsprobleme. Da eine große Anzahl der gängigen IP-PBX die Sicherheitsfeatures TLS und SRTP noch nicht unterstützen, können die Sprachpakete via VPN zur IP-PBX geleitet werden. In vielen Unternehmensbereichen gibt es heute VPN vor allem für die externen Nutzer, so dass Equipment und Know-how für diese Technologie schon vorhanden sind. Der positive Nebeneffekt für VoIP: Externe Büros lassen sich leicht an die Telefonanlage anbinden, ohne dass es lästige NAT-Probleme mit den dort installierten Routern gäbe. Während die Verschlüsselung durch VPN im Server kein großes Problem darstellt, sind Endgeräte mit VPN heute aber noch rar.

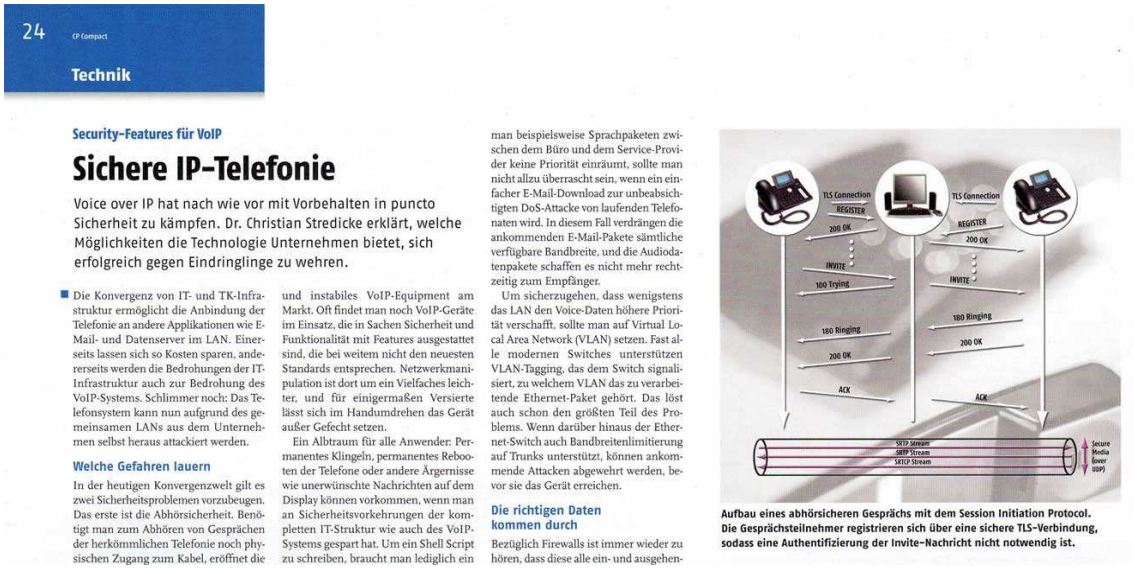
Will man bei VoIP den kompletten Datenschutz, funktioniert dieser nicht ohne TLS und SRTP. TLS, landläufig auch als „https“ bekannt, garantiert die Privatsphäre signalisierter Daten. Zudem verhindert es Man-in-the-middle-Attacken, in denen jemand vortäuscht, der Server zu sein. SRTP verschlüsselt die Sprachdatenpakete. Bei künftigen Projekten sollten

Kunden unbedingt darauf achten, dass Hard- und Software für TLS und SRTP zumindest geeignet sind und nicht durch einfache Maßnahmen zum Absturz gebracht werden können.

Proprietäre Sicherheitslösungen und Verschlüsselungstechniken sind für den Nutzer nicht nachvollziehbar. Daher ist bei dem Vergleich von Unternehmenslösungen darauf zu achten, dass offene und allgemeine Standards bei der Umsetzung von Sicherheitslösungen verwendet werden. Diese Lösungen basieren in der Regel auf den Protokollvereinbarungen SIPS und SRTP - offene Protokolle, die dank der Richtlinien der zentralen Standardisierungsorganisation für Internetprotokolle IETF nachvollzieh- und kontrollierbare Sicherheitsfeatures sind.

In Zusammenarbeit mit Dr. Christian Stredicke, snom Gründer und Vorstand

Erschienen in: ChannelPartner, VoIP-Spezial, 07.09.2007



24 CP Compact

Technik

Security-Features für VoIP

Sichere IP-Telefonie

Voice over IP hat nach wie vor mit Vorbehalten in puncto Sicherheit zu kämpfen. Dr. Christian Stredicke erklärt, welche Möglichkeiten die Technologie Unternehmen bietet, sich erfolgreich gegen Eindringlinge zu wehren.

Die Konvergenz von IT- und TK-Infrastruktur ermöglicht die Anbindung der Telefonie an andere Applikationen wie E-Mail- und Datenserver im LAN. Einerseits lassen sich so Kosten sparen, andererseits werden die Bedrohungen der IT-Infrastruktur auch zur Bedrohung des VoIP-Systems. Schlimmer noch: Das Telefonsystem kann nun aufgrund des gemeinsamen LANs aus dem Unternehmen selbst heraus attackiert werden.

Welche Gefahren lauern

In der heutigen Konvergenzwelt gilt es zwei Sicherheitsproblemen vorzubeugen. Das erste ist die Abhörsicherheit. Benötigt man zum Abhören von Gesprächen der herkömmlichen Telefonie noch physischen Zugang zum Kabel, eröffnet die und instabiles VoIP-Equipment am Markt. Oft findet man noch VoIP-Geräte im Einsatz, die in Sachen Sicherheit und Funktionalität mit Features ausgestattet sind, die bei weitem nicht den neuesten Standards entsprechen. Netzwerkmanipulation ist dort um ein Vielfaches leichter, und für einigermaßen Versierte lässt sich im Handumdrehen das Gerät außer Gefecht setzen.

Ein Albtraum für alle Anwender: Permanentes Klingeln, permanentes Rebooten der Telefone oder andere Ärgernisse wie unerwünschte Nachrichten auf dem Display können vorkommen, wenn man an Sicherheitsvorkehrungen der kompletten IT-Struktur wie auch des VoIP-Systems gespart hat. Um ein Shell Script zu schreiben, braucht man lediglich ein man beispielsweise Sprachpaketen zwischen dem Büro und dem Service-Provider keine Priorität einräumt, sollte man nicht allzu überrascht sein, wenn ein einfacher E-Mail-Download zur unbeabsichtigten DoS-Attacke von laufenden Telefonaten wird. In diesem Fall verdrängen die ankommenden E-Mail-Pakete sämtliche verfügbare Bandbreite, und die Audiodatenpakete schaffen es nicht mehr rechtzeitig zum Empfänger.

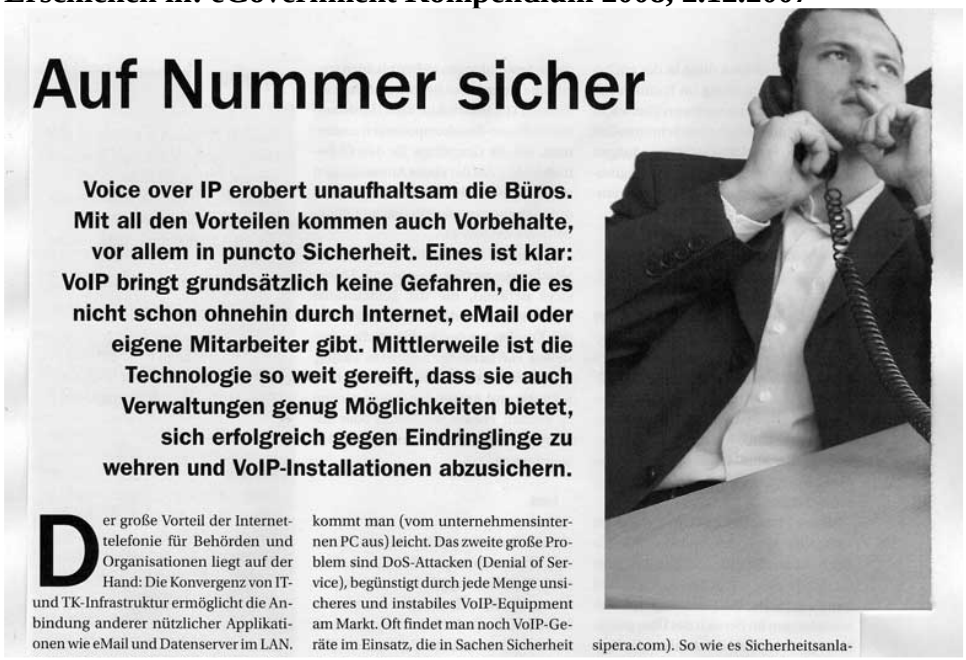
Um sicherzugehen, dass wenigstens das LAN den Voice-Daten höhere Priorität verschafft, sollte man auf Virtual Local Area Network (VLAN) setzen. Fast alle modernen Switches unterstützen VLAN-Tagging, das dem Switch signalisiert, zu welchem VLAN das zu verarbeitende Ethernet-Paket gehört. Das löst auch schon den größten Teil des Problems. Wenn darüber hinaus der Ethernet-Switch auch Bandbreitenlimitierung auf Trunks unterstützt, können ankommende Attacken abgewehrt werden, bevor sie das Gerät erreichen.

Die richtigen Daten kommen durch

Bezüglich Firewalls ist immer wieder zu hören, dass diese alle ein- und ausgehen-

Aufbau eines abhörsicheren Gesprächs mit dem Session Initiation Protocol. Die Gesprächsteilnehmer registrieren sich über eine sichere TLS-Verbindung, sodass eine Authentifizierung der Invite-Nachricht nicht notwendig ist.

Erschienen in: eGovernment Kompendium 2008, 2.12.2007



Auf Nummer sicher

Voice over IP erobert unaufhaltsam die Büros. Mit all den Vorteilen kommen auch Vorbehalte, vor allem in puncto Sicherheit. Eines ist klar: VoIP bringt grundsätzlich keine Gefahren, die es nicht schon ohnehin durch Internet, eMail oder eigene Mitarbeiter gibt. Mittlerweile ist die Technologie so weit gereift, dass sie auch Verwaltungen genug Möglichkeiten bietet, sich erfolgreich gegen Eindringlinge zu wehren und VoIP-Installationen abzusichern.

Der große Vorteil der Internettelefonie für Behörden und Organisationen liegt auf der Hand: Die Konvergenz von IT- und TK-Infrastruktur ermöglicht die Anbindung anderer nützlicher Applikationen wie eMail und Datenserver im LAN. kommt man (vom unternehmensinternen PC aus) leicht. Das zweite große Problem sind DoS-Attacken (Denial of Service), begünstigt durch jede Menge unsicheres und instabiles VoIP-Equipment am Markt. Oft findet man noch VoIP-Geräte im Einsatz, die in Sachen Sicherheit sipera.com). So wie es Sicherheitsanla-