

Sichere IP-Kommunikation

Thomas Romer
IP Communications Manager
Avaya



Unternehmen setzen zur Optimierung ihrer Kommunikation zunehmend auf IP-basierte konvergente Netzwerke. Dies stellt jedoch neue Anforderungen an die Absicherung der Infrastrukturen, die es zu bewältigen gilt.

IT-Verantwortliche in der Pflicht

Attacken gegen Netzwerke und Anwendungen, die den Geschäftsbetrieb oder die Vertraulichkeit von Firmen- und Mitarbeiterdaten gefährden, sorgen immer wieder für Aufsehen. Es werden mehr und mehr Angriffe verzeichnet. Diese Entwicklung belegen auch von dem CERT Coordination Center und dem ISC (International Information Systems Security Certification Consortium) vorgelegte Studien. Demzufolge nahm die Zahl sicherheitsrelevanter Vorfälle von 1999 bis 2003 von 10000 auf 130000 zu und stieg damit um das 3,4-fache schneller als die im gleichen Zeitraum entstandenen Internet-Hosts. Diese Statistiken sind jedoch weit von der alltäglichen Realität entfernt, die oftmals anders aussieht. Darüber hinaus spiegeln sie nicht das Ausmass des Schadens wieder, den Attacken hervorrufen. So ist das unberechtigte Abwickeln von externen Telefongesprächen auf Kosten von Unternehmen ein lukratives Geschäft. Der daraus resultierende Verlust belief sich gemäss einer von der CFCA (Communications Fraud Control Association) durchgeführten Studie im Jahr 2003 weltweit auf etwa 35 bis 40 Milliarden US-Dollar. Die wesentlichen Gründe hierfür sind zum einen in der zunehmenden Anzahl von Schwachstellen in Anwendungen zu sehen, zum anderen in dem geringeren Know-how, das Angreifer für die Durchführung von Attacken benötigen. IT-Verantwortliche müssen sich somit vermehrt der Aufgabe stellen, nicht nur ein reines Daten-, sondern ein konvergentes Netzwerk abzusichern.

Technologie als strategischer Erfolgsfaktor

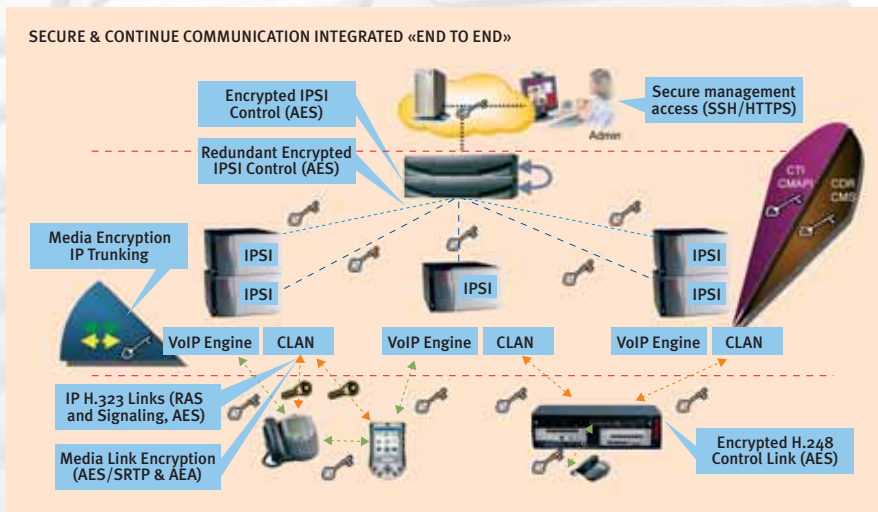
Die stetig voranschreitende globale wirtschaftliche Vernetzung und der damit einhergehende Trend zur Virtualisierung, zwingt Unternehmen umzudenken. In diesem veränderten Umfeld stellt der Einsatz neuer Technologien einen strategischen Erfolgsfaktor dar. Um ihre Wettbewerbsfähigkeit zu stärken, entscheiden sich Konzerne daher immer häufiger dafür, separat betriebene Sprach- und Datennetzwerken durch eine einzige Infrastruktur zu ersetzen. Dies erleichtert die Einführung konvergenter Kommunikationslösungen, die gerade im Hinblick auf die Steigerung der Kundenzufriedenheit eine wichtige Rolle spielen. Des Weiteren ermöglicht der Betrieb einer einheitlichen auf Internetprotokoll-Technologien basierenden Netzinfrastruktur die Zusammenführung von Sprach- und Unternehmensanwendungen wie zum Beispiel Enterprise Resource Planning (ERP) und Supply Chain Management (SCM). Dies eröffnet



zahlreiche neue Optionen, wie beispielsweise die Einbindung von Kommunikationsanwendungen in Workflow-Management-Programme oder die Bereitstellung von Lösungen, deren Verfügbarkeit die Mobilität der Mitarbeiter steigert. Die Realisierung konvergenter Netzwerke und die Nutzung integrierter Kommunikationslösungen wirken sich somit positiv auf die Unternehmenseffizienz aus und verringern die für das IT-System aufzuwendenden Gesamtbetriebskosten deutlich.

Konvergente Infrastrukturen umfassend schützen

Doch hiermit erhält auch die Absicherung von Kommunikationsanwendungen einen neuen Stellenwert. Denn traditionelle IT-Sicherheitslösungen, die sich in erster Linie auf den Schutz reiner Datennetzwerke beschränken, greifen bei konvergenten Infrastrukturen nicht länger. Vielmehr bedarf es der Umsetzung zusätzlicher Massnahmen, um Risiken bei der Übertragung von Sprache auszuschalten und Applikationen keinerlei Gefahren auszusetzen. Integrierte Sprach-Daten-Anwendungen, hierzu zählen beispielsweise Multimedia-Contact Center-, Unified-Communication-, Messaging- oder Interactive Voice-Response-Lösungen, müssen somit künftig ebenfalls bei der Planung von Sicherheitsstrategien berücksichtigt werden.



Die bittere Realität in Zahlen

Gemäss einer aktuellen von Avaya in Auftrag gegebenen europaweiten Studie ist dies jedoch nicht unbedingt die Regel: Während 90% der befragten Unternehmen Sicherheitsrichtlinien für ihr Datennetzwerk bereits implementiert haben, trifft dies im Hinblick auf Sprachapplikationen nur auf 44% zu. Zudem überprüfen nur 24% der untersuchten Organisationen mindestens einmal im Quartal, ob ihre bestehenden Richtlinien weiterhin angemessen sind. Trotz der alarmierenden Situation führten im Vorjahreszeitraum darüber hinaus nur ein Drittel der im Rahmen der Studie berücksichtigten Firmen umfassende Risikoanalysen durch. Erschreckend auch, dass Verantwortliche viele Sicherheitsverstösse erst dann erkennen, wenn sie von Aussenstehenden darauf aufmerksam gemacht werden oder es eigentlich schon zu spät ist, also Angriffe bereits aufgetreten sind und es in der Folge zu Ausfällen kommt. Dies lässt sich nur so erklären, dass bei der Unternehmensführung immer noch eine mangelnde Sensibilität in Sachen IT Security – dies betrifft besonders die Absicherung der zum Einsatz kommenden Systeme – an der Tagesordnung ist. Ebenso sind Budgetbeschränkungen als Grund dafür anzusehen, dass Infrastrukturen nur unzureichend geschützt sind.

Vertraulichkeit steht an erster Stelle

Sicherheit sollte demzufolge bei der Umstellung auf IP-Telefonie zu den Top-Prioritäten zählen. Umfassende Lösungen werden in diesem Kontext aber nur von wenigen Herstellern in der Art offeriert, wie Avaya sie bietet. Aus unserer Sicht sollte die Einführung von IP-Telefonielösungen beim Kunden stets davon begleitet sein, dass ein höheres Vertraulichkeits- und Sicherheitsniveau erzielt wird. Um dies zu gewährleisten, stützt Avaya bereits seit geraumer Zeit sein gesamtes zur Auslieferung kommendes Spektrum an IP-

Endgeräten mit sicheren Authentifikations- und Media-Encryption-Technologien aus. Auf diese Weise sind Gespräche in jeder anzunehmenden Situation bestens geschützt, zusätzliche Kosten entstehen hierfür nicht. Kunden erhalten so die Möglichkeit weitgehend risikolos von den zahlreichen Vorteilen zu profitieren, die konvergente Lösungen bieten. Die ebenfalls integrierte Verschlüsselung der Steuersignalisierung aller im Portfolio verfügbaren IP-Telefone und Media Gateways, die den Anschluss von digitalen/analoge Nebenstellen und der Amtsverbindung gewährleisten, verhindert die Manipulation und das Aufzeichnen vertraulicher Gesprächsinformationen. Ausserdem werden die über das Telefon übermittelten Passcodes für die Benutzeranmeldung, Autorisierungscode für Amtsleitungen sowie zum Beispiel über das Telefon übermittelte Kreditkarteninformation geschützt. Ein sicherer Verwaltungszugriff mittels OTP- (One Time Password) Authentisierung inklusive umfassender Überwachungsfunktionalitäten und eine starke Verschlüsselung dieser Verbindungen gehören zum Sicherheitsstandard, mit denen Avaya alle angebotenen konvergenten Kommunikationsanwendungen ausstattet. Die Security und Business Continuity Features stellen nur zwei der zahlreichen Unterscheidungsmerkmale dar, die IP-Telefonie-Anwendungen von Avaya von anderen Lösungen dieser Kategorie abheben. Die Bereitstellung eines umfassenden Spektrums an Sicherheitsmassnahmen ist in jedem Fall für Unternehmen ein Muss, die künftig auf eine sichere und verlässliche IP-Kommunikation vertrauen möchten.

Die Absicherung des konvergenten Sprach-Daten-Netzwerks stellt derzeit jedoch für IT-Verantwortliche noch eine Herausforderung dar, die aber mit Hilfe eines guten Partners zu meistern ist.

Sämtliche Avaya-Lösungen werden in der Schweiz durch die Firma Telekom & Netzwerk AG betrieben und implementiert.

TELEKOM & NETZWERK AG

8305 Dietlikon
Industriestrasse 2

8047 Zürich
Flüelastrasse 32

4552 Derendingen
Spechtweg 12A

1023 Crissier
Chemin de Cloislet 20

Tel. 0844 835 356
info@t-n.ch
www.t-n.ch