

Sichere IP Communications

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) hat zur „Systems“ einen Bericht zur Sicherheit bei der IP Communications herausgebracht, der viele Kunden aufhorchen lässt.

Sie planen in ihrem Unternehmen die, bisherige Telefonanlage durch eine deutlich günstigere und effiziente IP-Telefonie-Infrastruktur abzulösen oder haben dies bereits getan? So weit, so gut. Haben Sie dabei aber auch die Sicherheit im Blick? IP- Kommunikation erfordert die Absicherung gegen Angriffe jeder Art, die mit der Zeit zunehmend komplexer und umfangreicher geworden sind. Die Lösung von Cisco Systems sichert dementsprechend mit zahlreichen Maßnahmen alle Bereiche der intelligenten IP-Infrastruktur: Switches, Router, Endgeräte, Datenbanken, Verzeichnisse, Server und Applikationen. Dabei spielt die Authentifizierung der verwendeten Geräte, die Autorisation der Nutzer und der intelligente Schutz der Server eine wesentliche Rolle.

Mit dem Siegeszug der IP- Technologie wird auch IP- Telefonie zunehmend zum Standard in Unternehmensnetzwerken. Verunsichert durch die Vielzahl von aktuellen Sicherheitsvorfällen, die teilweise zum Ausfall ganzer Unternehmensnetzwerke geführt ha-



BSI warnt vor mangelnder Sicherheit bei VoIP (25.10.2005)

Die unbedachte Einführung von Voice-over-IP bringt erhebliche Bedrohungspotenziale mit sich, warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in der zur Systems vorgestellten Studie [VoIPSec](#). Noch seien keine "spektakulären Angriffe" bekannt geworden, doch dies sei nur eine Frage der Zeit.

Die Studie des BSI ist für Leser interessant, die sich in die Materie einarbeiten wollen, gibt's sie doch einen guten Überblick über Technologie, Angriffsszenarien und Gegenmaßnahmen.

„Geeignete Sicherheitsmaßnahmen [im Umfeld von Voip] sind heute technisch und organisatorisch realisierbar. Allerdings unterstützt nur ein Bruchteil der aktuell auf dem Markt befindlichen Systeme die erforderlichen Sicherheitsmaßnahmen im erforderlichen Umfang. Bei der Auswahl eines Systems sollten daher die realisierten Sicherheitsmaßnahmen im Fokus stehen und nicht nur reine Funktionalitätsgesichtspunkte in die Entscheidung einbezogen werden.“ (VoIPSec) Andererseits seien Abhörtools wie Vomit (Voice over misconfigured Internet Telephones) für SIP beziehungsweise H.323-Plug-ins für den Ethernet-Sniffer Ethereal weit verbreitet. Vomit ermöglicht ein Mitschneiden der Gesprächsinhalte, Ethereal erlaubt das Ausspähen von Ziel- und Quelladresse.

Dies hat Cisco Systems bereits seit Jahren erkannt und entsprechende Leistungsmerkmale in Switches, Router, Gateways,

ben, stellen Unternehmen hohe Sicherheitsanforderungen an IP-Telefonie-Lösungen. Dabei ist die Sprache im IP-Netz ebenso vielen Bedrohungen ausgesetzt wie in der klassischen, analogen oder ISDN-Telefonie. In der alten Telefonwelt werden Gespräche in der Regel nicht verschlüsselt und können beispielsweise relativ leicht durch das Anklemmen an die Verkabelung abgehört werden. Telefonie-Betrug (Fraud) oder die Vortäuschung fremder Identitäten zur Erschleichung von Dienstzugängen sind dort ebenso möglich wie Denial-of-Service-Angriffe. Diese haben Sie vermutlich selbst schon erlebt, wenn Sie eine gut frequentierte Service Hotline angerufen haben und nicht durchgekommen sind.

Unabhängig davon, ob sich ein solcher Vorfall in der klassischen Welt oder in der IP-Telefonie-Welt ereignet – die Konsequenzen für das Unternehmen sind gravierend. Nicht-Erreichbarkeit bedeutet Vertrauensverlust, stört die Kundenbindung und kann schließlich in Umsatzausfällen und Imageverlust münden. Ebenso ist unerheblich, ob vertrauliche Finanz-, Personal- oder Strategieinformationen das Unternehmen als EMail oder als Sprache verlassen – werden sie abgefangen, ist der Schaden der Gleiche.

Soft-PBX (Callmanager) und Endgeräten implementiert. Die entsprechende Sicherheitsarchitektur ist seit dem gewachsen, Tools für deren Management wurden bereitgestellt und damit betrieblich handhabbar.

Cisco's Infrastruktur überlebte einen gross angelegten Hacker-Test der „Mierkom“ 2004 als einziger Hersteller unbeschadet, bei dem Marktweit Hersteller von VoIP geladen waren. Seit dem hat Cisco Systems seine VoIP-Sicherheitsarchitektur sogar noch weiterentwickelt und steht auch in diesem Aspekt mit Abstand führend im Markt.

Auf der Website von Cisco Systems sind seit Jahren detaillierte Anleitungen (bis auf Konfigurationslevel herab) für jeden downloadbar, wie Sicherheit bei der IP-Communication praktisch umsetzbar ist.

Das BSI empfiehlt aus verfahrenstechnischen Gründen „entsprechend freigegebene IP-Verschlüsselungs-Gateways“ für Verschlusssachen-Kommunikation. Hier kann Cisco Systems mit entsprechenden Geräten unterstützen.

Bereits seit Mai 2005 ist der Cisco „Callmanager“ BSI-zertifiziert (BSI-PP-0012-2005 conformant Common Criteria Part 2 conformant), was die äußerst frühen Anstrengungen Cisco's verdeutlicht. (<http://www.bsi.bund.de/zertifiz/zert/reporte/0306a.pdf>)

Folgende kurze Übersicht soll einige der sicherheitsrelevanten Merkmale VoIP- Sicherheitsinfrastruktur Cisco's verdeutlichen

Angriffe auf Telefonie an sich:

- Passwortenforcment
- Multi- Level Administration
- Schutz des Serverbetriebssystems durch den Cisco Security Agent
- Redundanz aller Kommunikationsinfrastrukturelemente
- Gehärtete Betriebssysteme – offene, proaktive Kommunikation bei aufgedeckten Sicherheitsrisiken
- Verschlüsselung aller Web-zugriffe von Usern und Admin's
- Verschlüsselung auf fast allen Endgeräten und Gateways
- Authentifizierung von Endgeräten, Softswitchen und Gateways auch gegeneinander
- Autorisierung
- Signierung der Images (für Telefone bspw.)
- QoS als Sicherheitsmerkmal (DDoS)
- Logging
- Alarmgenerierung
- Managementeinbindung

Angriffe auf das Datennetzwerk (Switching):

- Dynamische MAC- Sicherheit
- Verhindern von MAC- Spoofing
- diversen DHCP- Angriffen
- Angriffen auf den Spanning Tree
- VLAN- Angriffen
- Multicast- Angriffen
- Private VLANS
- MAC Adresslisten- Filter
- Integrierte Firewall's, SSL- Gateways und Load- Balancer in den Switchen
- L3- Funktionalitäten in Switchen
- Authentifizierungsmechanismen (u.a. 802.1x)
- QoS als Sicherheitsmerkmal (DDoS)
- Logging
- Alarmgenerierung
- Managementeinbindung

Angriffe auf das Datennetzwerk (Routing):

- Access- Listen
- Authentifizierung diverser Protokolle (Zugriff, Routing, Access)
- QoS
- Intelligente integrierte Firewalls (SIP/Skinny/H.323)
- Application Layer Gateways
- QoS als Sicherheitsmerkmal (DDoS)
- Logging
- Alarmgenerierung
- Managementeinbindung
- Integration von Routing- und Gatewayfunktionalitäten
- Integration von Routing- und Applikations- Funktionalitäten (Voicemail, VXML, Voice- Roting, Überlebens-telefonie)

Fazit:

Cisco ist der Marktführer bei sicherer VoIP und IP Communications. In diversen Zertifikaten (inkl. des BSI's selbst) und Tests schlägt sich das nieder. Das ist auch nicht weiter verwunderlich, da Cisco Systems als erster Datentechnik- Hersteller überhaupt Sicherheitsmerkmale in die IP- Communications integrierte.

Die Sicherheitsmerkmale sollten bei der Kaufentscheidung noch vor den Leistungsmerkmalen an erster Stelle rangieren. Ein schlecht gesichertes System kann seine auch noch so guten Leistungsmerkmale bei Versagen (Angriff, Netzausfall) nicht mehr bereitstellen.

Wir beraten Sie gerne bei technischen Fragen und stellen unser praktisch erworbenes Wissen aus 10 Jahren Voice over IP bei vielen Kundenprojekten bereit.

CISCO SYSTEMS



Weitere Informationen:

http://wwwin-emea.cisco.com/bus_dev/germany/content/technologie_loesungen/AVVID/Produktinformationen/IPTelefonie_ist_sicher.pdf

<http://www.cisco.com/safe/>