

# IP-TELEFONIE IST SICHER



## DIE VOIP-TOPOLOGIE

Cisco Systems trägt den Anforderungen nach mehr Sicherheit in Voice-over-IP-Netzwerken Rechnung und bietet für alle Bereiche einer VoIP-Infrastruktur umfassende Sicherheitsmaßnahmen. Zu dieser Umgebung zählen:

- Endgeräte wie IP-Telefone sowie PCs und Server.
- Eine Infrastruktur mit Switches, Routern oder dedizierten Appliances.
- Eine Server-Architektur, auf der unter anderem die zentrale Software zur Anrufsignalisierung – der Cisco CallManager – läuft.

Als Marktführer im Bereich IP Networking bietet Cisco die Expertise und ein umfassendes Konzept für sichere IP-Telefonie.



Ihr Unternehmen plant, seine bisherige Telefonanlage durch eine deutlich günstigere und effiziente IP-Telefonie-Infrastruktur abzulösen oder hat 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 haben, 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 E-Mail oder als Sprache verlassen – werden sie abgefangen, ist der Schaden der Gleiche.

## **INTEGRIERTE SICHERHEIT ERLEICHTERT DEN UMSTIEG**

Eine umfassende, unternehmensweite Sicherheitsrichtlinie ist die Grundlage für alle weiteren technischen Maßnahmen. Die technische Umsetzung sollte ebenfalls einen ganzheitlichen Ansatz verfolgen, also Sicherheitsfunktionen durchgehend im gesamten Netzwerk integrieren und diese exakt aufeinander abstimmen. Die Grundfunktionen zur Absicherung bietet Ihr Netzwerk in den meisten Fällen bereits: Cisco Switches und Router sind über das Cisco IOS-Betriebssystem schon mit den grundlegenden Sicherheitsfunktionen ausgestattet. Diese zu aktivieren, verursacht kaum zusätzliche Kosten und bietet integrierte Sicherheit im gesamten Netzwerk. Damit ist die Grundlage für sichere IP-Telefonie geschaffen.



## **BUFFER OVERFLOW**

Angreifer nutzen im Falle eines Buffer Overflow einen Programmierfehler bei der dynamischen Speicherreservierung für Variablen aus. Steht zu wenig Speicher zur Verfügung und kommen zu viele Daten an, läuft der reservierte Puffer über. Dabei werden wichtige Rücksprungsadressen überschrieben und der Programmcode des Angreifers auf Rechnern abgelegt. Die CPU führt deshalb statt des regulären Rücksprungs den Programmcode des Angreifers aus. So erlangt er die volle Kontrolle über einen fremden Rechner.

## **EIN SICH SELBST SCHÜTZENDES NETZ**

Die Vision von Cisco für die Absicherung von Netzwerken hat einen Namen: Self-Defending Network. Diese Strategie basiert auf den drei Säulen Sicherer Transport, Abwehr von Angriffen und Bedrohungen sowie dem Trust- und Identitätsmanagement. Die Strategie findet ihre Anwendung auch in der Absicherung von IP-Telefonie-Infrastrukturen mit Virtual LANs (VLAN), die die Sprach- von der Datenebene trennen. Sie dämmen beispielsweise Gefahren wie Denial-of-Service-Angriffe ein, da nicht beide Ebenen mit Anfragen überflutet werden. Neben VoIP-fähigen Firewalls kommen Access Control Lists (ACLs) zum Einsatz. Sie kontrollieren den Zugriff zwischen Sprach- und Daten-VLANs, basierend auf IP-Adresse sowie Protokoll- und Port-Informationen des anfragenden Teilnehmers. Auf der Datenebene kommen Softphones wie der Cisco IP Communicator zum Einsatz. Diese Endnutzer-Workstations sind in der Regel Viren- und Würmerangriffen ausgesetzt. Werden Funktionen wie Intrusion Detection und ACLs auf Komponenten wie Routern, Switches, Servern und Clients (PCs) implementiert, sind Sicherheitsmaßnahmen damit integraler Bestandteil der gesamten Infrastruktur. Firewalls sitzen an strategischen Punkten, beispielsweise an Übergangspunkten von der Sprach- zur Datenebene. Damit sind die separaten Netzwerke intelligent und sicher miteinander verbunden.

## **STRATEGISCHE ABWEHR MIT VOIP-FÄHIGEN FIREWALLS**

Die Übergänge zwischen den verschiedenen Sprach- und Datennetzwerksegmenten und natürlich zum Internet werden mit Voice-over-IP-fähigen Firewalls geschützt. Die Cisco PIX Firewall Security Appliance ist eine echte Application-Layer Firewall, die Stateful-Inspection und Network-Address-Translation für die VoIP-Signalisierung bietet. Neben H.323 (einschließlich Version 4) und Skinny werden auch SIP (Session Initiation Protocol) und MGCP (Media Gateway Control Protocol) unterstützt. So wird sichergestellt, dass das Unternehmensnetzwerk keinen unnötigen Risiken durch offene Ports zum Internet ausgesetzt ist. Die Firewall – auf den Cisco Routern und Switches auch als IOS Firewall verfügbar – überwacht die Signalisierung und öffnet immer nur die Ports, die aktuell benötigt werden. Mit Firewalls wie der Cisco PIX 506 oder 515 und in Kombination mit Virtual Private Networks (VPN) können Unternehmen Sprach- und Multimediadienste sicher auf Niederlassungen oder Home Offices erweitern. Cisco hat zudem mit V3PN eine Lösung für den sicheren Transport von Sprache und Video über IPsec-VPN (IP Security) entwickelt, mit dem sich sogar Service-Level für verschlüsselte Sprachübertragung garantieren lassen.

## **SICHER WIE EIN FELS IN DER BRANDUNG**

Dass die IP-Telefonie-Lösung und die zugrunde liegende Netzwerk-Infrastruktur von Cisco sicher sind, hat im Mai 2004 ein Test von Miercom, einem Mitglied der Network World Lab Alliance, ergeben. Cisco hat mit der Bestnote „Sicher“ abgeschlossen – selbst fortgeschrittene Hacker konnten nicht in die Voice-Architektur von Cisco eindringen oder sie nennenswert stören. Die Testumgebung mit dem CallManager 4.0 entsprach dem Cisco-Lösungsansatz SAFE. Das System konnte sich gegen das eines anderen Herstellers durchsetzen. Weitere Hersteller nahmen am Test gar nicht erst teil. Den vollständigen Artikel können Sie unter [www.nwfusion.com](http://www.nwfusion.com) abrufen.

## EIN AGENT FÜR IHRE SICHERHEIT

Das Herzstück der IP-Kommunikations-Lösung von Cisco, der Cisco CallManager, ist mit dem Cisco Security Agent (CSA) for IP Communications ausgestattet. Der CSA schützt Anwendungen auf Servern wie Cisco CallManager, Cisco Unity Unified

Communications, Cisco Personal Assistant und Cisco IP Contact Center (IPCC) Express. Er härtet das Betriebssystem und überwacht Anwendungen permanent. Mit Hilfe einer Positivliste (Sicherheitspolicy) überprüft der CSA, welche Aktionen einer Anwendung erlaubt sind. Dies hat den Vorteil, dass nicht bei jedem Sicherheitsvorfall das Regelwerk aufgefrischt werden muss, wie es bisher beispielsweise bei Antivirus- oder IDS-Produkten der Fall ist. Mit dem CSA sind zahlreiche Gefahren wie die Ausnutzung von Buffer Overflows bereits gebannt. Der Cisco Security Agent fasst viele verschiedene Sicherheitsfunktionen in einer Software zusammen – verteilte Personal Firewall, Host-basiertes Intrusion-Prevention-System, Schutz vor gefährlichem mobilen Code, Betriebssystem-Integrität und Audit-Log-Konsolidierung. Dadurch sinken die Betriebskosten deutlich.

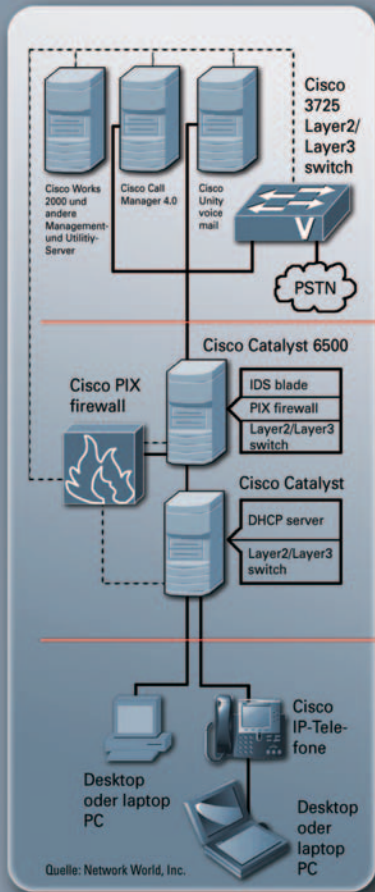
Der CallManager verfügt über weitere Sicherheitsfunktionen, um die Identität der Geräte und Server, mit denen er kommuniziert, zu identifizieren (siehe Kasten „Digitale Zertifikate im IP-Telefon“). Er unterstützt zudem die Verschlüsselung von Anrufsignalen und Mediastreams.

## AUTHENTIFIZIERUNG UND NETZWERKZUGANGSKONTROLLE

Nur wenn die Identität eines Gerätes im Netzwerk zweifelsfrei feststellbar ist, sollte die Teilnahme am Netzwerk autorisiert werden. Deshalb sind digitale Zertifikate ein wesentlicher Bestandteil des Cisco VoIP-Sicherheitskonzeptes. IP-Telefone und der Cisco CallManager authentifizieren sich gegenseitig mit Hilfe von X.509v3-Zertifikaten. Um durchgehende Sicherheit zu gewährleisten, gilt die gleiche Forderung - „nur zweifelsfrei identifizierte Geräte dürfen in das Netzwerk“ - auch für das Datennetzwerk. Deshalb stehen auch hier starke Authentifizierungsfunktionen mit digitalen Zertifikaten zur Verfügung. Der Industriestandard 802.1x sorgt im LAN dafür, dass nur Endgeräte mit gültigem Zertifikat in das Netzwerk hinein gelassen werden. So geschützt lassen sich mit Softphones ausgestattete PCs oder Laptops zum Telefonieren oder für Videokonferenzen nutzen und die Flexibilität von IP-basierter Telefonie wird voll ausgeschöpft.

Doch Authentifizierung und digitale Zertifikate sind nur ein erster Schritt. Cisco hat im Rahmen seiner Self-Defending-Network-Strategie die Lösung Network Admission Control (NAC) entwickelt, um diese Sicherheitsmaßnahmen noch zu erweitern. Cisco NAC prüft, ob Endgeräte das geforderte Sicherheitsniveau haben, bevor sie Zugang zum Netzwerk erhalten. Über eine spezielle Schnittstelle, den Cisco Trust Agent (CTA), wird das Sicherheitsniveau der Endgeräte abgefragt, beispielsweise Patchlevel des Betriebssystems oder der Status des Antivirus-Tools. Ein zentraler Richtlinienserver kann dann entscheiden, ob das Gerät den Anforderungen entspricht oder ob es in Quarantäne genommen wird. So werden wirkungsvoll Sicherheitsrisiken identifiziert und isoliert. Es entsteht kein weiterer Schaden.

### VoIP-Topologie = Maximale Sicherheit



#### VoIP-Infrastruktur

- Cisco Security Agent auf allen Servern
- Mit Firewalls geschützter Out-of-Band-Management-Zugriff auf alle Server und Infrastruktur-Geräte
- Umfassendes Monitoring aller sicherheitsrelevanten Aktivitäten

#### Netzwerk-Infrastruktur

- Integrierter Denial-of-Service-Schutz in den Switches mit Cisco IOS, inklusive Rate Limiting
- Dynamic Address Resolution Protocol Inspection; weitere Cisco IOS Sicherheitsmaßnahmen
- Firewalls an strategischen Punkten
- Separate Sprach- und Daten-VLANs

#### Endgeräte-Ebene

- Authentifizierung mit Zertifikaten, verschlüsselte VoIP-Verbindungskontrolle und -signalisierung
- IP-Telefone 7940, 7960 und 7970 mit digitalen Zertifikaten
- Cisco Security Agent auf Desktops oder Laptops
- Lokale IP-Telefon-Administration

### DIGITALE ZERTIFIKATE IM IP-TELEFON

Das IP-Telefon Cisco 7970 wird direkt ab Werk mit einem digitalen Zertifikat (MIC – Manufacturer Installed Certificate) ausgestattet. Bereits vorhandene IP-Telefone 7940, 7960 oder 7970 können vom Betreiber nachträglich mit einem digitalen Zertifikat (LSC – Locally Significant Certificate) ausgestattet werden. Dies geschieht mit der in den CallManager 4.0 integrierten CAP-Funktion (Certificate Authority Proxy). Betreiber können per CAPF selbst digitale Zertifikate erzeugen oder eine bereits vorhandene, unternehmenseigene Private Key Infrastruktur (PKI) oder die Dienste eines externen Zertifikatsdienstes nutzen. Die PKI regelt alle Prozesse zur Bereitstellung von elektronischen Signaturen.

## DIE VORTEILE DER CISCO-LÖSUNG AUF EINEN BLICK

- Eine umfassende und ganzheitliche Sicherheitslösung
- Technologie und Expertise vom Marktführer im Bereich IP Networking
- Bestehende Sicherheitsfunktionen können ohne Zusatzkosten aktiviert werden
- Keine zusätzlichen Investitionen für Sicherheitsupdates auf den Servern auf Grund des Cisco Security Agent
- Zukunftsweisendes Sicherheitskonzept
- Bestätigte Sicherheit durch unabhängigen Test
- Unterstützung aller gängigen Verschlüsselungs- und Authentifizierungsmechanismen
- Ausfallsicherheit durch Redundanz

## CISCO SYSTEMS GESCHÄFTSSTELLEN:

Cisco Systems GmbH  
Am Söldnermoos 17  
85399 Hallbergmoos  
Tel: (01 80) – 3 67 10 01  
Fax.: (0811) – 55 43-10

Cisco Systems GmbH  
Industriestraße 3  
65760 Eschborn  
Tel: (01 80) – 3 67 10 01  
Fax: (0 61 96) – 77 39-700

Cisco Systems GmbH  
Hansaallee 249  
40549 Düsseldorf  
Tel: (01 80) – 3 67 10 01  
Fax: (02 11) – 5 20 29-010

Cisco Systems GmbH  
Herold Center  
Am Wilhelmsplatz 11  
70182 Stuttgart  
Tel: (01 80) – 3 67 10 01  
Fax: (07 11) – 2 39 11-11

Cisco Systems GmbH  
Kurfürstendamm 21-22  
10719 Berlin  
Tel: (01 80) – 3 67 10 01  
Fax: (030) – 9 78 92-110

Cisco Systems GmbH  
Neuer Wall 77  
20354 Hamburg  
Tel: (01 80) – 3 67 10 01  
Fax: (040) – 37 67-44 44

[www.cisco.de](http://www.cisco.de)

## WIE SICHER DARF ES SEIN? ABHÖRSICHER?

Vielfach hat sich die Vorstellung etabliert, das Internet sei unsicher. Und da IP-Telefonie über das Internet-Protokoll läuft, sei auch IP-Telefonie unsicher. Dies ist ein weit verbreiteter Irrtum, denn IP-Telefonie kann über das Unternehmensnetzwerk nicht nur sicher, sondern auch vertraulich abgewickelt werden. Hierzu stehen für die IP-Telefone 7940, 7960 und 7970 Authentifizierungsmechanismen zur Verfügung. Ein Teil der IP-Telefone von Cisco unterstützt zudem starke Verschlüsselungsmechanismen. Die Signalisierung wird per TLS (Transport Layer Security) geschützt, die Sprache selbst mit dem leistungsfähigen SRTP (Secure Realtime Transport Protocol). So gesichert lassen sich die Kostenvorteile bei der Nutzung des Internets als kostengünstige Transportplattform beruhigt voll ausschöpfen.

## AUSFALLSICHER

Redundanz ist beim Aufbau einer IP-Telefonie- oder IPCC-Infrastruktur ein wesentliches Kriterium, da sie den geschäftsschädigenden Ausfall der Sprach-Infrastruktur verhindert. Mehrere Cisco CallManager können hierzu in einem Cluster als eine Einheit betrieben und verwaltet werden. Durch eine dreifache CallProcessing-Server-Redundanz wird eine exzellente Systemverfügbarkeit erreicht. Einem IP-Telefon stehen damit außer seinem primären CallManager noch bis zu zwei weitere BackUp CallManager Server in seiner Konfiguration zur Verfügung. Bei einem eventuellen Ausfall des primären Servers registriert sich das Cisco IP-Telefon automatisch bei dem nächsten BackUp Server. Da der Cisco CallManager nur für die Signalisierung von Telefongesprächen notwendig ist, würde es auch bei einem Serverausfall nicht zum Abbruch des Telefongesprächs kommen.

Eine sehr hohe Ausfallsicherheit bietet auch die Cisco Survivable Remote Site Telephony (SRST). Hierbei können in den Außenstellen eines Unternehmens die Cisco IOS Router, die auch die Anbindung an das öffentliche Sprachnetz durchführen, das gesamte CallProcessing der IP-Telefone in der Außenstelle übernehmen, falls es zu einem Ausfall der Anbindung an die Zentrale kommen sollte. Damit würde der Kontakt zu dem zentralen CallManager unterbrochen werden und die IP-Telefone in der Außenstelle würden sich automatisch an dem lokalen Cisco IOS Router registrieren und damit betrieben werden. Diese Ausfallsicherung bewahrt Unternehmen vor fatalen wirtschaftlichen Folgen.

## SICHERE IP-KOMMUNIKATION

Mit der Kombination all dieser Sicherheits- und Redundanzmaßnahmen auf Basis einer Security-Policy können Unternehmen ihre IP-Kommunikations-Infrastruktur wirkungsvoll und ohne hohen Investitionsaufwand absichern. Cisco bietet mit SAFE einen umfassenden Ansatz, der die IPT-Sicherheitsfunktionen in die gesamte Sicherheitsarchitektur des Unternehmens einbettet. Über viele dieser Sicherheitsmaßnahmen verfügt Ihr Netzwerk bereits. Informieren Sie sich! Weltweit profitieren bereits über 14.500 Unternehmen mit mehr als drei Millionen IP-Telefonen von der neuen und sicheren Technologie.

Weitere Informationen zu den Sicherheitslösungen von Cisco Systems finden Sie unter: [www.cisco.com/safe](http://www.cisco.com/safe) und [www.cisco.com/go/voice](http://www.cisco.com/go/voice)