

## 2M05: Sicherheit von IP-Telefonie

Referent:

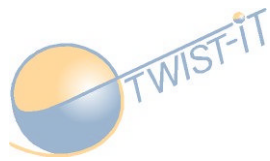
**Christoph Bronold**

BKM Dienstleistungs GmbH

© 2006 BKM Dienstleistungs GmbH

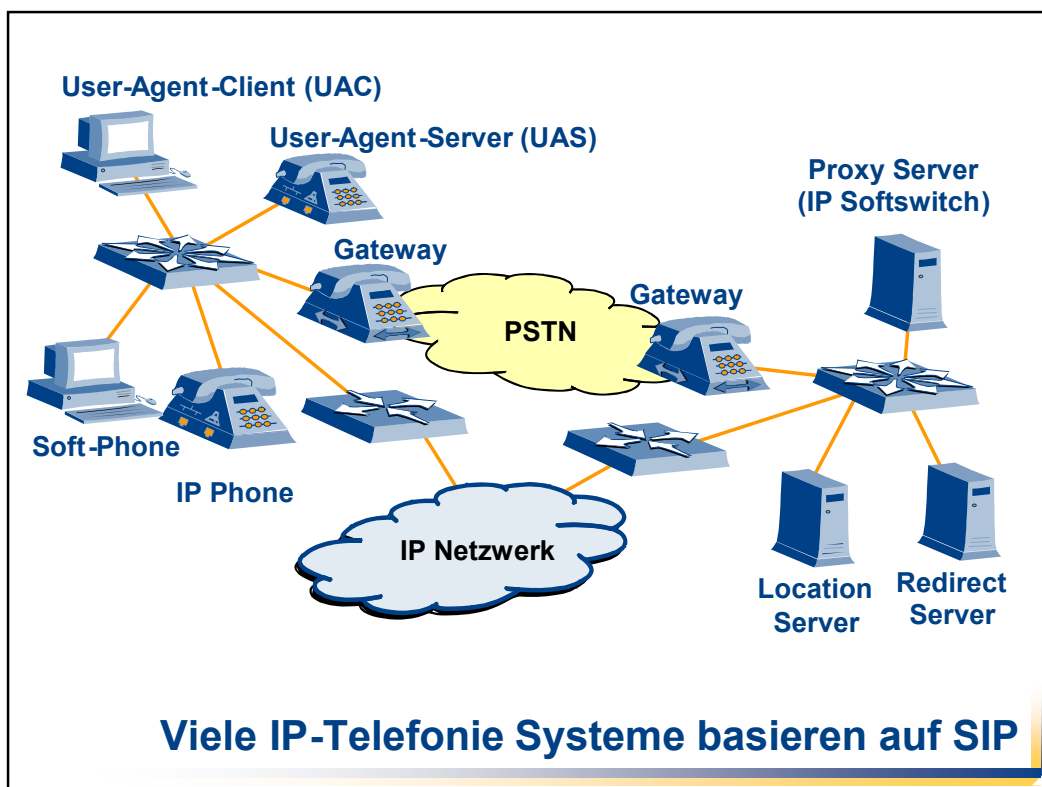
- **Bedrohungen und Angriffe auf IP-Telefonie Systeme**
- **Sicherheitsmaßnahmen für IP-Telefonie Systeme**
- **Best-Practices**
- **Designrichtlinien für sichere IP-Telefonie Systeme**

**Agenda**



## Bedrohungen und Angriffe auf ein IP-Telefonie System

© 2006 BKM Dienstleistungs GmbH



**➤ Bedrohungen:**

- ▶ Abhören von IP Telefongesprächen
- ▶ Fälschung der Identität des Anrufers
- ▶ Fälschung der Identität des Angerufenen
- ▶ Veränderung des Status von Endgeräten
- ▶ „Lahm legen“ des IP Telefons
- ▶ Kostenlos oder auf Kosten anderer telefonieren
- ▶ SPIT (Spam over Internet Telephony) Anrufe

**➤ Angriffe:**

- ▶ Manipulation der Zugangsdaten
- ▶ DoS Attacken auf IP Telefon oder PC mit Soft-Phone
- ▶ Auslesen der Netzwerk-Konfiguration vom IP Telefon
- ▶ Exploits gegen die IP Telefonieapplikation



**Bedrohungen und Angriffe: IP Telefon**

**➤ Bedrohungen:**

- ▶ „Lahm legen“ der IP Telefonanlage
- ▶ Ausspionieren von Zugangsdaten und Abrechnungsdaten
- ▶ Manipulation der Eingangzeitpunkt von Nachrichten (Voice Mail etc.)
- ▶ Manipulation von Registrierungs- und Lokalisierungsinformationen
- ▶ Änderung des Status eines Rufes

**➤ Angriffe:**

- ▶ Manipulation der Signalisierungsdaten
- ▶ DoS Attacken gegen das Betriebssystem (Windows/Linux)
- ▶ Exploits gegen die IP Telefonieapplikation
- ▶ Viren oder Trojaner auf den Server einschleusen



**Angriffsziel: IP Telefonanlage**

**➤ Bedrohungen:**

- ▶ Hacker möchte Datenpakete von fremden Stationen mit abhören und/oder manipulieren (Man-in-the-Middle Attack)
- ▶ „Lahm legen“ des Netzwerks

**➤ Angriffe:**

- ▶ CAM Table Overflow
- ▶ VLAN Hopping (Switch Spoofing, Double Tagging)
- ▶ Spanning-Tree Protocol (STP) Manipulation/Angriffe
- ▶ MAC Spoofing/ARP Spoofing
- ▶ Private VLAN Attacks

**Bedrohungen und Angriffe: Layer 2 Netzwerk****➤ Bedrohungen:**

- ▶ Hacker möchte das Netzwerk zu seinem Gunsten manipulieren
- ▶ Einschleusung von eigenen Systemen

**➤ Angriffe:**

- ▶ DHCP Starvation/Rogue DHCP Server
- ▶ Routing Protocol Attack/Manipulation/Route Injection
- ▶ HSRP- und VRRP Angriffe
- ▶ ICMP Redirect
- ▶ IRDP Spoofing
- ▶ IP Spoofing

**Bedrohungen und Angriffe: Layer 3 Netzwerk**

➤ **Bedrohungen:**

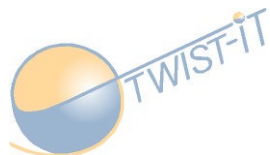
- ▶ Hacker möchte das Netzwerk zu seinem Gunsten manipulieren
- ▶ Einschleusung von eigenen Systemen
- ▶ "lahm legen" von IP-Telefonie Systemen und Netzwerken

➤ **Angriffe:**

- ▶ SYN Flood
- ▶ Ping Flood
- ▶ Malware Angriffe (Viren, Würmer, Trojaner etc.)
- ▶ Exploits
- ▶ DNS Spoofing
- ▶ Password Sniffing



**Bedrohungen und Angriffe: Layer 4 - 7 Netzwerk**



**Sicherheitsmaßnahmen für  
IP-Telefonie Systeme**

### ➤ Authentisierung von SIP Nachrichten:

- ▶ HTTP Digest (RFC 2617/RFC 3261)

### ➤ Verschlüsselung von SIP Nachrichten:

- ▶ S/MIME (RFC 3851 Version 3.1)
  - Nur SDP Body (= Inhalt einer SIP Nachricht)



- ▶ TLS 1.0 (RFC 2246)

- Sicherheit auf der Transportschicht



- ▶ IPsec (RFC 2401 ff.)

- Sicherheit auf der Netzwerkschicht

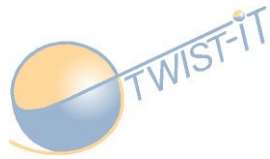


## Sicherheitsmaßnahmen für SIP-basierte Telefonie

### ➤ The Secure Real-time Transport Protocol (SRTP) (RFC 3711):

- ▶ Schlüsselmanagement
  - z.B. Multimedia Internet Keying (MIKEY)
- ▶ Verschlüsselung
  - AES-CTR (128 Bit Blöcke)
  - AES-f8
- ▶ Authentifikation und Integrität
  - HMAC-SHA1 (nur 80 Bits von 160 Bits verwendet)

## Sicherheitsmaßnahme für Spracheübertragung



## Best-Practices

© 2006 BKM Dienstleistungs GmbH

- **Verschlüsselung der Gespräche**
- **Authentifizierung**
  - ▶ Primäre Authentifizierung erfolgt über MAC Adresse
  - ▶ MAC Adressen können gespoofed sein
  - ▶ Einige IP Telefone haben Basis-Authentifizierung durch anmelden am Telefon (nur 4-stellige PIN)
  - ▶ Jeder Benutzer benötigt einen Usernamen und Passwort
- **PC-basierte IP Telefonie-Software ist unsicher**
  - ▶ PC ist immer verletzbar (OS, Applikationen, Softphone)
  - ▶ Keine VLAN-Trennung von Sprache und Daten möglich
- **Getrennte VLANs für Sprache und Daten**

## Best-Practices: IP Phones

- **Automatische Registration von unbekanntem IP Telefonen abschalten**
- **Aktivierung einer Firewall:**
  - ▶ Nur bekannte VoIP Stationen (IP Hard-/Soft-Phone, Gateways, etc.) zulassen
  - ▶ Anzahl der Management Stationen einschränken und Zugriff nur über SSH/HTTP/IPsec erlauben
- **Immer alle Security-Patches einspielen**
- **Alle unnötigen Services im Server ausschalten**
- **Installation von HIDS und Security Agents auf den Servern**
- **Redundante Systeme**

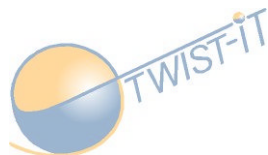
### **Best-Practices: IP Softswitch**

- **Separates VLAN für Daten und Sprache**
  - ▶ Private VLAN optional für Sprache
  - ▶ Separate VLANs für IP Telefone und Gatekeeper und Voice-Mail System
  - ▶ Deaktivierung von nicht benutzten Ports an den Ethernet Switches
- **Authentifizierung der Stationen mittels IEEE 802.1x**
- **Implementierung von Quality of Service:**
  - ▶ DiffServ
  - ▶ Call Admission Control (Bandbreitenüberwachung mit RSVP)
- **NIDS/NIPS zur Erkennung und Abwehr von Angriffen**
- **IPsec für die sichere Übertragung über das LAN**
- **Redundante System (Switch, Router, etc.)**

### **Best-Practices: Netzwerk**

- **Firewall trennt IP Telefone vom IP Softswitch ab**
  - ▶ Jeder Voice Traffic soll durch die Firewall gehen (zwischen IP Telefon und IP Softswitch)
  - ▶ Filterung des Traffics zum Voice-Mail System
- **Firewall muss stateful Filterung von Voice Traffic unterstützen:**
  - ▶ RTP benutzt UDP mit einem großem Portnummernbereich, der bei einer stateless Firewall freigegeben werden muss
- **Application Level Gateway (ALG)**
  - ▶ Parser für H.323, SIP, MGCP, SDP etc.

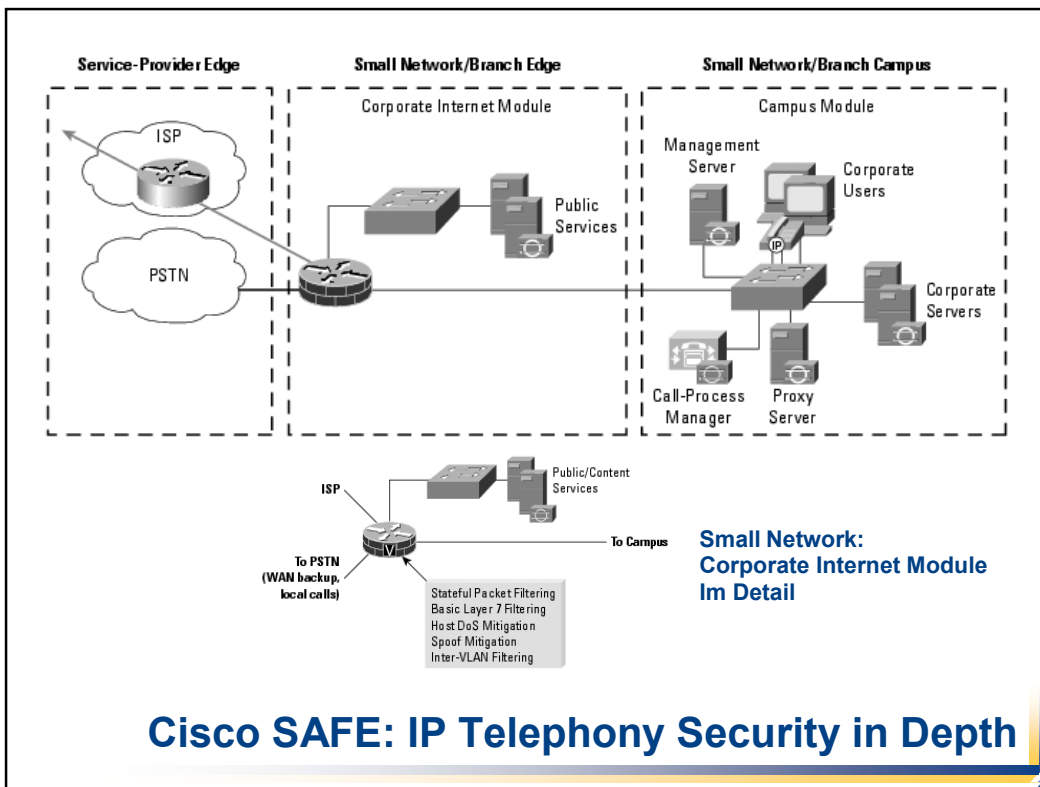
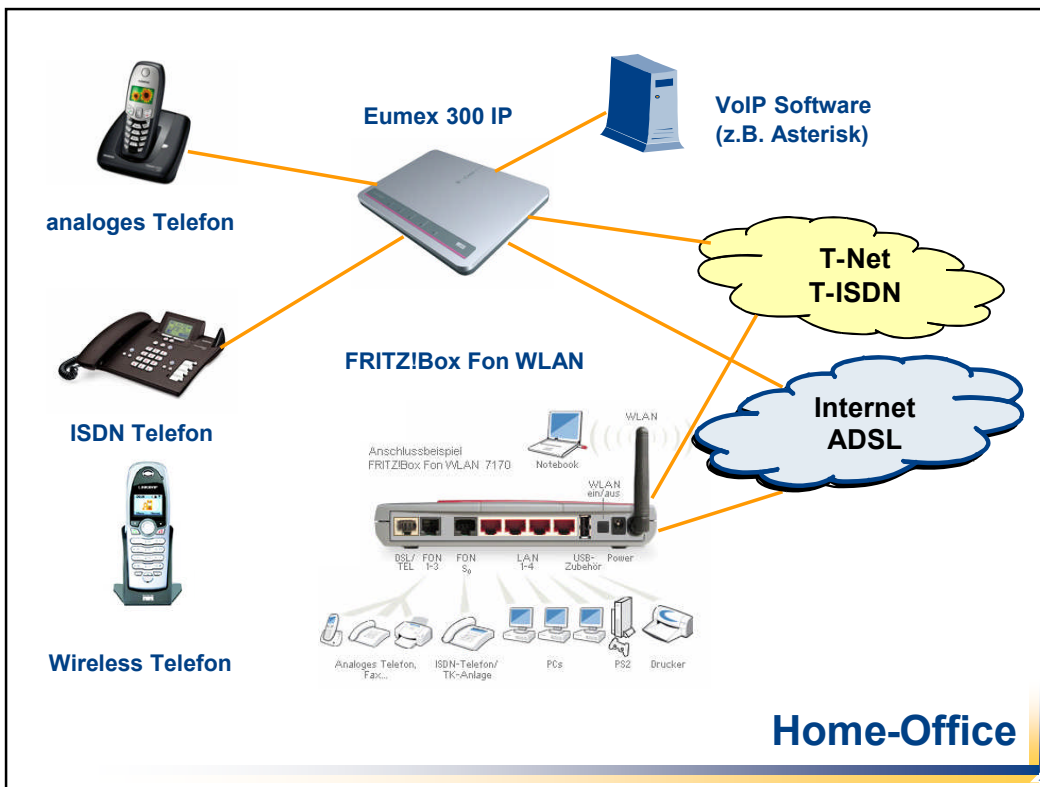
**Best-Practices: Firewall**

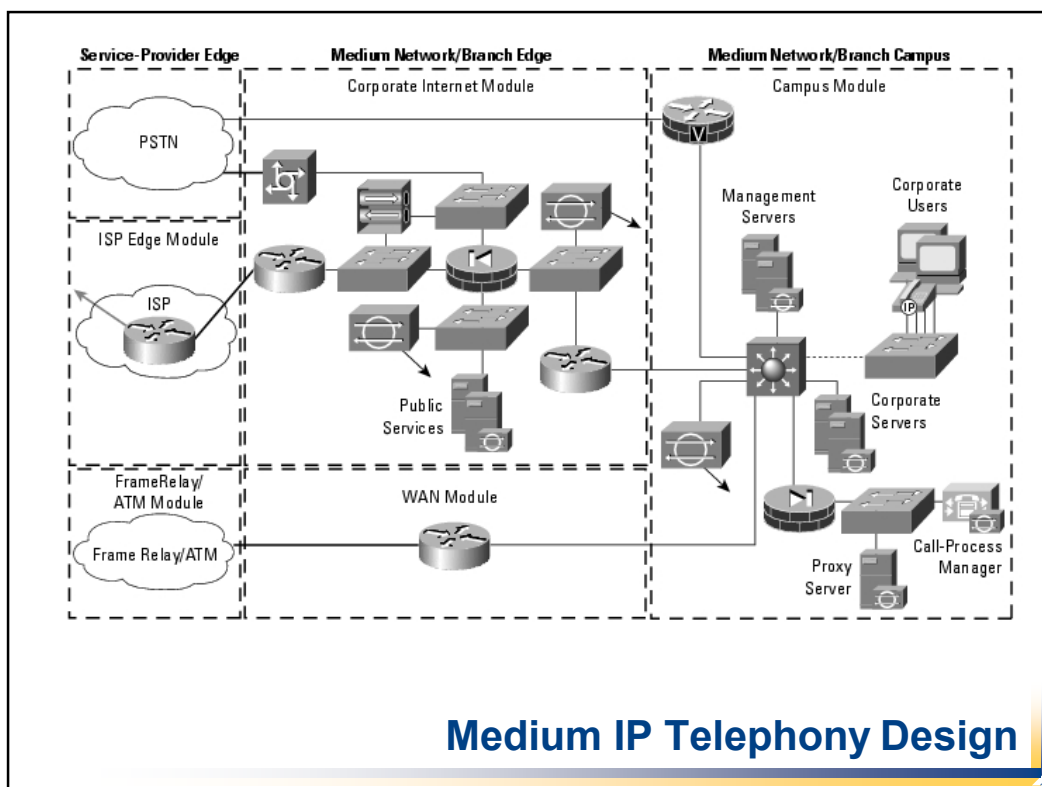
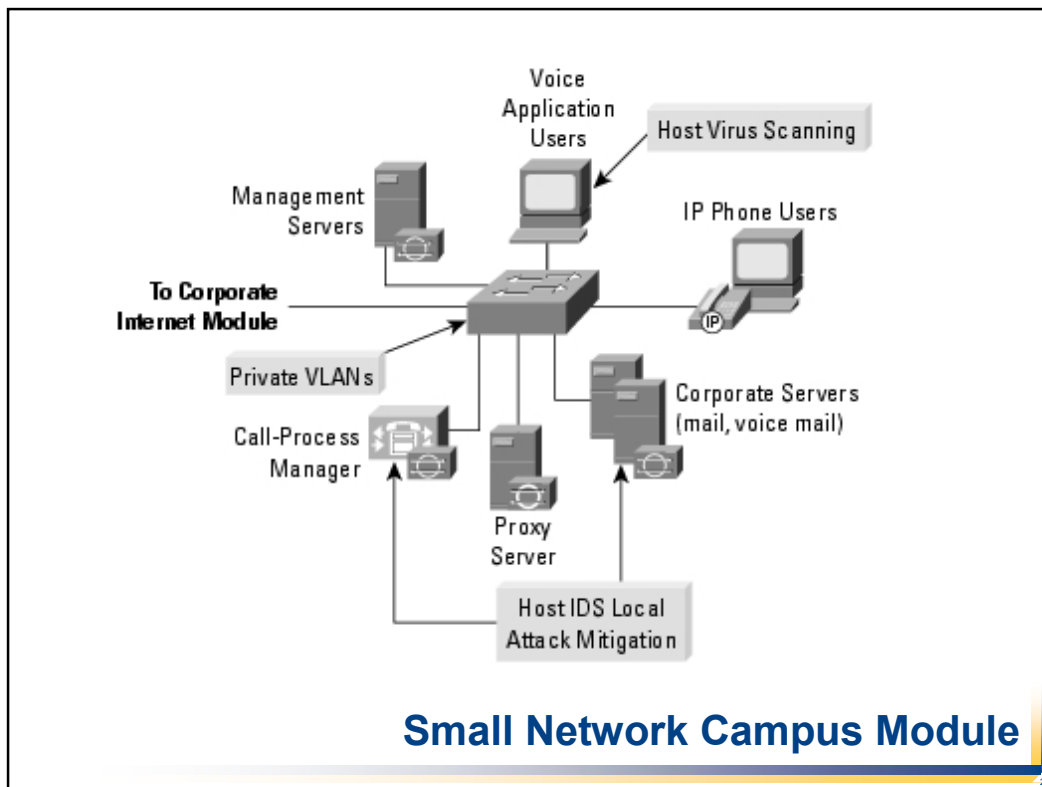


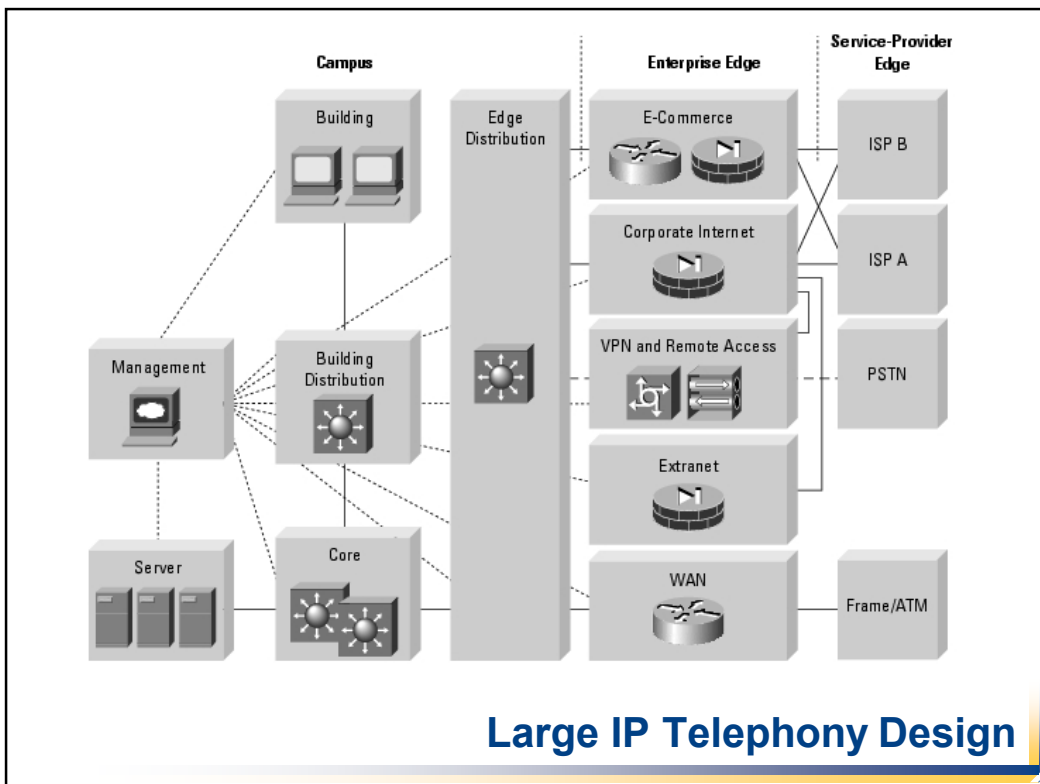
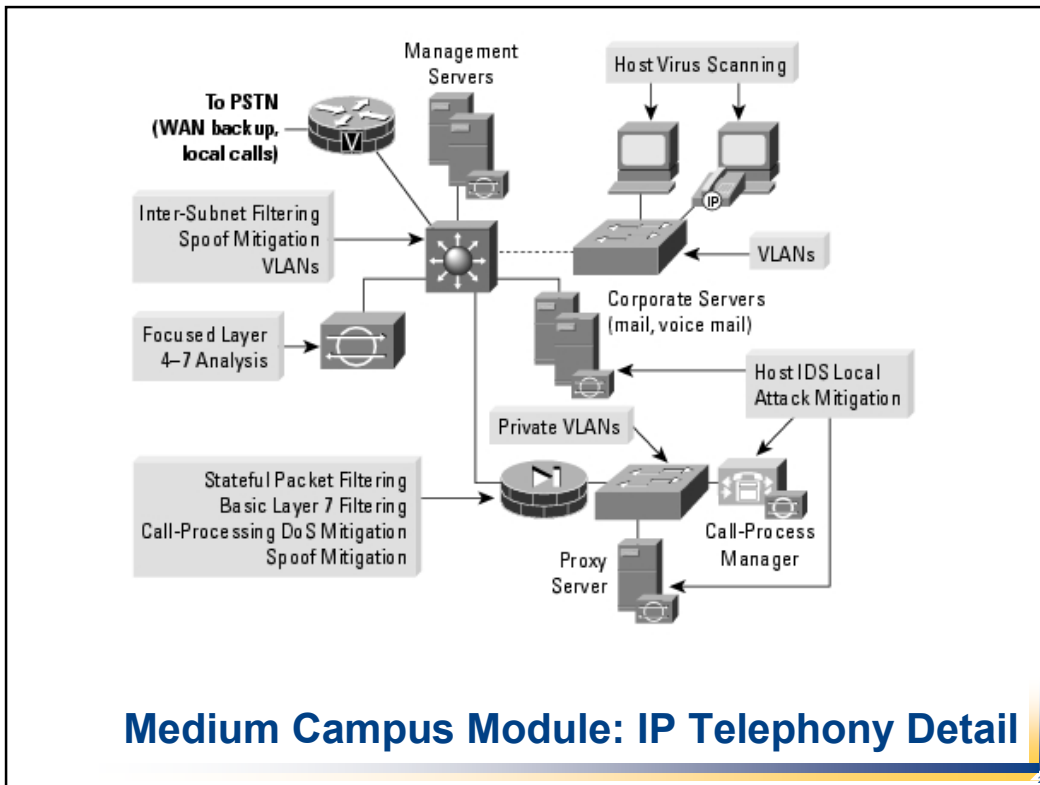
## **Designrichtlinien für sichere IP-Telefonie Systeme**

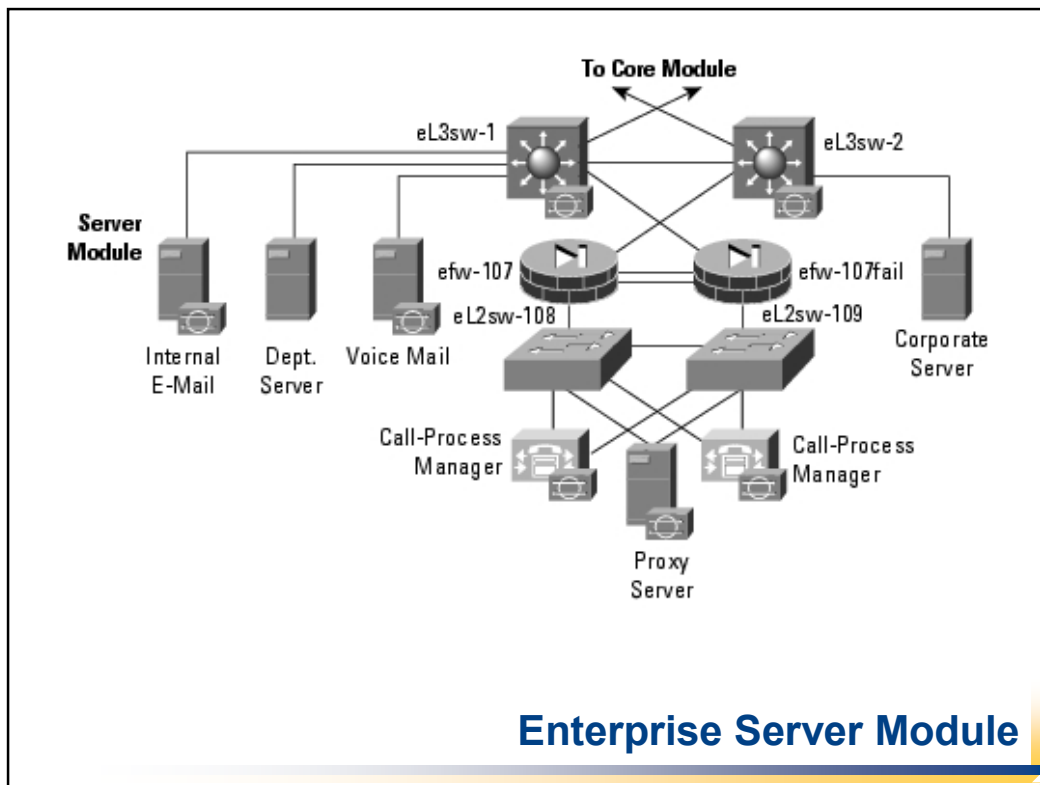
- **Home-Office (Heimarbeitsplatz/Privat)**
- **Small-Business (Kleine + mittlere Unternehmen)**
- **Large Enterprise (Große Unternehmen)**

© 2006 BKM Dienstleistungs GmbH









- **Bundesamt für Sicherheit in der Informations-technik (BSI): VoIPSEC - Studie zur Sicherheit von Voice over Internet Protocol**  
<http://www.bsi.de/literat/studien/VoIP/index.htm>
- **Cisco SAFE: IP Telephony Security in Depth:**  
<http://www.cisco.com/go/safe>
- **Breaking through IP telephony:**  
<http://www.nwfusion.com/reviews/2004/0524voipsecurity.html>
- **VoIP Security Alliance**  
<http://www.voipsa.org/>

**Referenzen/Links**



**Christoph Bronold**  
Christoph.Bronold@bkm-gmbh.com

**BKM Dienstleistungs GmbH**  
Hauptstrasse 5  
D-83607 Holzkirchen  
www.bkm-gmbh.com