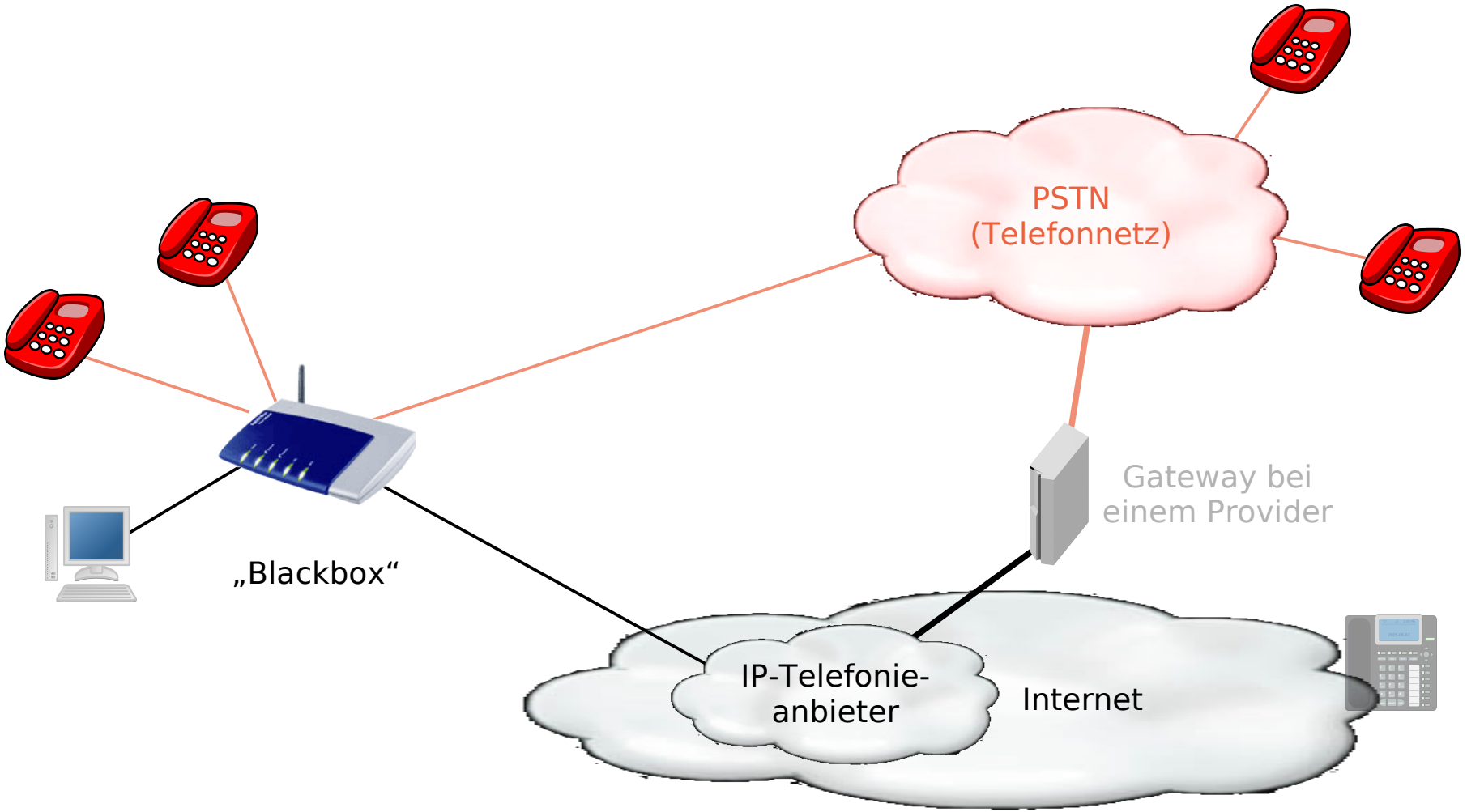
Internet-Telefonie
Mehr als billig Telefonieren

Hartmut Goebel
Diplom-Informatiker
IT-Security in komplexen Umgebungen

Goebel CONSULT

Spannend für zu Hause

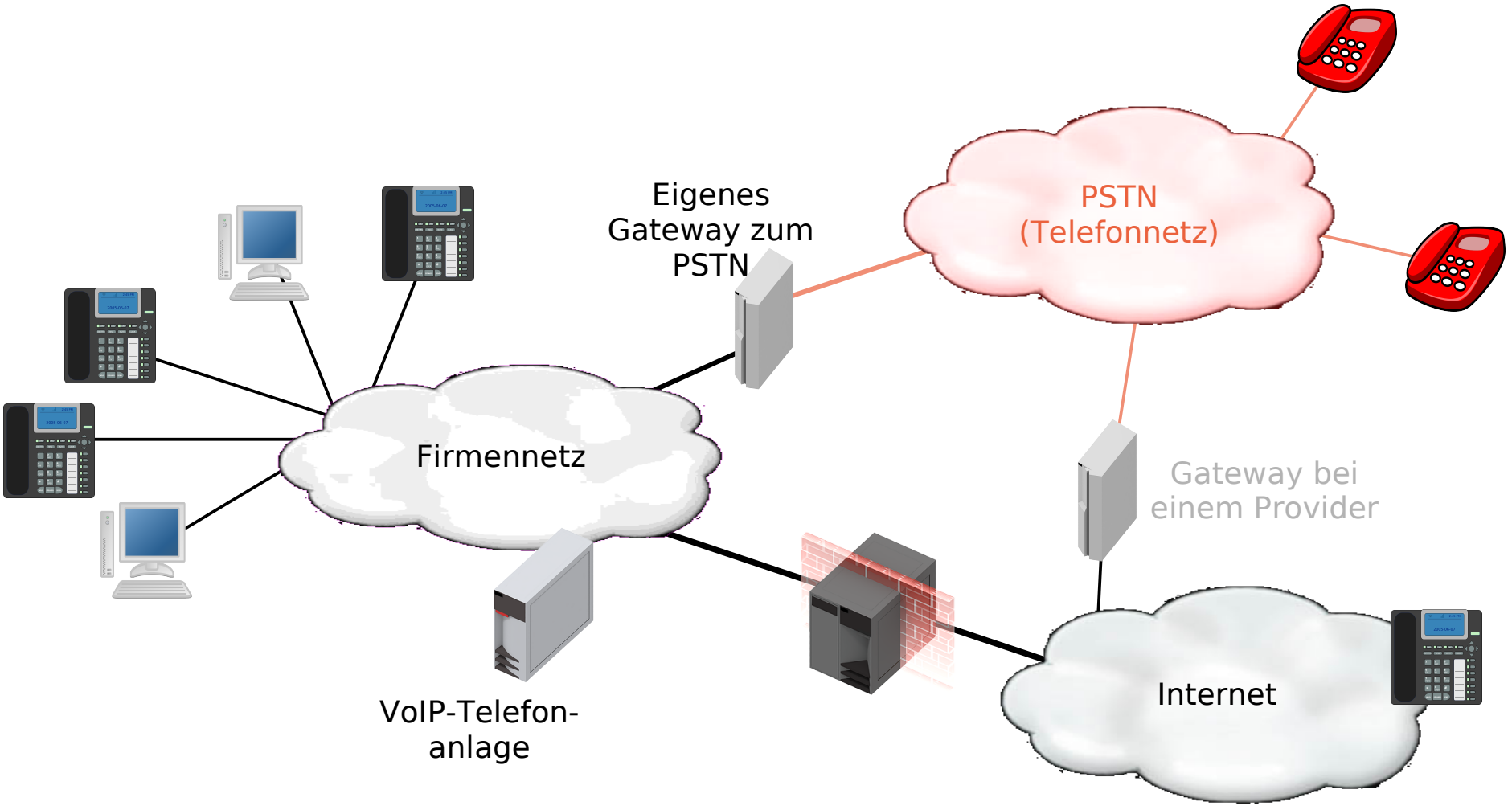
Internet-Telefonie



Goebel CONSULT

Standardlösung

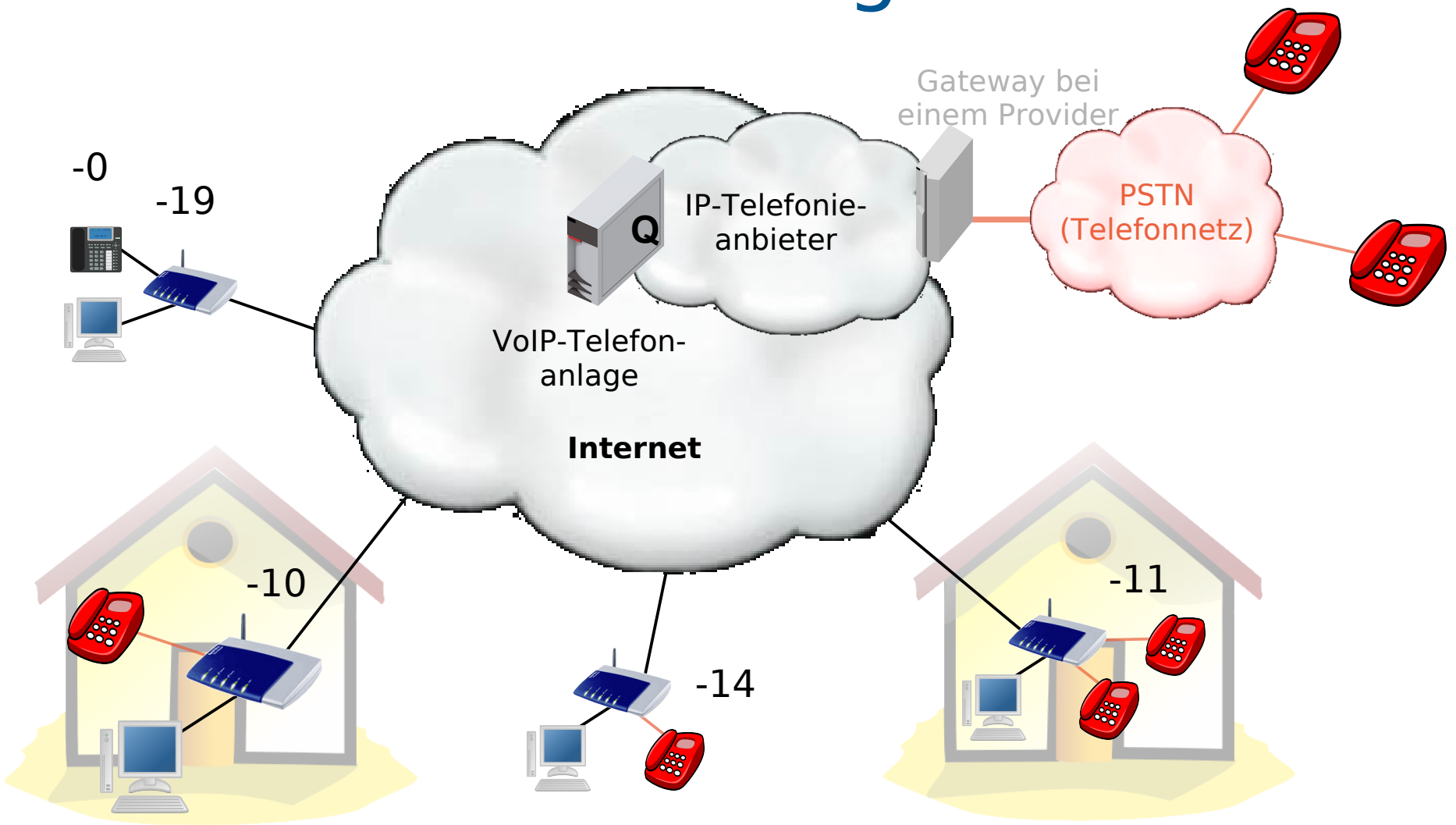
VoIP-Telefonie nur im Unternehmen



Goebel CONSULT

Für virtuelle Unternehmen

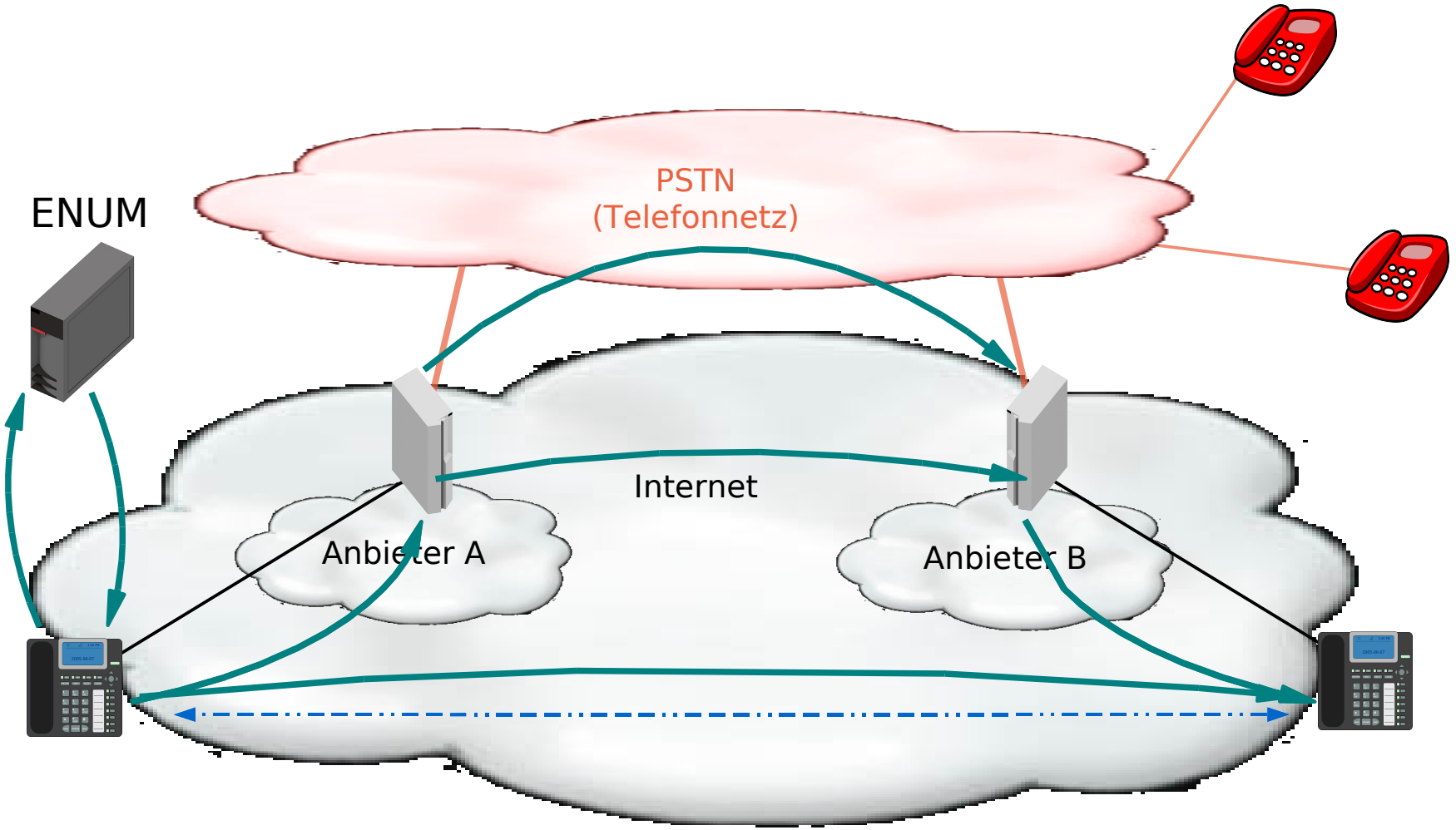
Virtuelle Telefonanlage



Goebel CONSULT

Es ginge auch dezentral

Womit Provider ihr Geld verdienen



ENUM

Von der Telefonnummer zum IP-Telefon

- Problem: Telefone haben nur Zifferntasten
- PSTN 0911 / 1234 - 11
- VoIP 11 @ 10.12.14.16
  meier @ telefon.meier-kg.de
- Lösung: DNS-Einträge
  - mehrere Ziele pro Nummer möglich
  - Datenschutz-Problem

Was wir vom Telefon gewöhnt sind

- funktioniert
- angezeigte Nummern stimmen
- wird nicht abgehört
- wird nicht protokolliert

➔Telefonie ist unternehmenskritisch

➔VoIP muss genau so zuverlässig sein

➔neue Herausforderung für IT-Leute (?)

Typische Gefährdungen

- Stromausfall
- Fehlbedienung
- Vorsätzliches Handlungen
  - Abhören, "Neugierige" Mitarbeiter
  - Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
  - Gebührenbetrug
  - Gefährdung bei Administrierungsarbeiten

➔ Unterschied: Jetzt ist das IT

Bedrohungen auf Anwendungs-Ebene

- Endgeräte
  - partieller Beeinträchtigung bis zu
  - vollständigen Übernahme der Kontrolle über das Gerät
- Middleware (Gateway, Gatekeeper, ...)
  - alle dadurch geleiteten IP-Telefonate gestört, abgehört, umgeleitet und manipuliert werden
  - --> Angreifer wird diese angehen
- Ursachen: Programme mit Schadfunktion, Implementierungsfehler Lücken im OS

Ein paar Schwachstellen im CallManager

Cisco CallManager Express SIP User Directory Disclosure: Exposure of sensitive information, from local network	2006-08-03 
Cisco Unified CallManager Multiple Vulnerabilities: Privilege escalation, DoS, System access, from remote	2006-07-13 
Cisco CallManager RealVNC Password Authentication Bypass: Security Bypass, from remote	2006-06-23 
Cisco CallManager Web Interface Cross-Site Scripting Vulnerabilities: Cross Site Scripting, from remote	2006-06-20 
Cisco CallManager Connection Handling Denial of Service: DoS, from local network	2006-01-19 
Cisco Call Manager CCMAdmin Privilege Escalation: Security Bypass, from local Network	2006-01-19 

Quelle und Einstufung: Secunia

Sicherheitsmaßnahmen (3)

Maßnahmen gegen Abhören

- Basisdienste: HTTPS, SSH (sic!)
- SRTP einsetzen, besser noch Zphone
- Bei H.323: Integritätsprüfung und Verschlüsselung
- Bei SIP: TLS aktivieren
- Endgeräte restriktiv konfigurieren
- Verschlüsselung für MPLS-Wolke

Noch Fragen?

Goebel Consult

IT-Security in komplexen Umgebungen

www.goebel-consult.de
h.goebel@goebel-consult.de