Security und VoIP

Ing. Herbert Putz

WIR SIND DIE GUTEN

www.inode.at

Ing. Herbert Putz

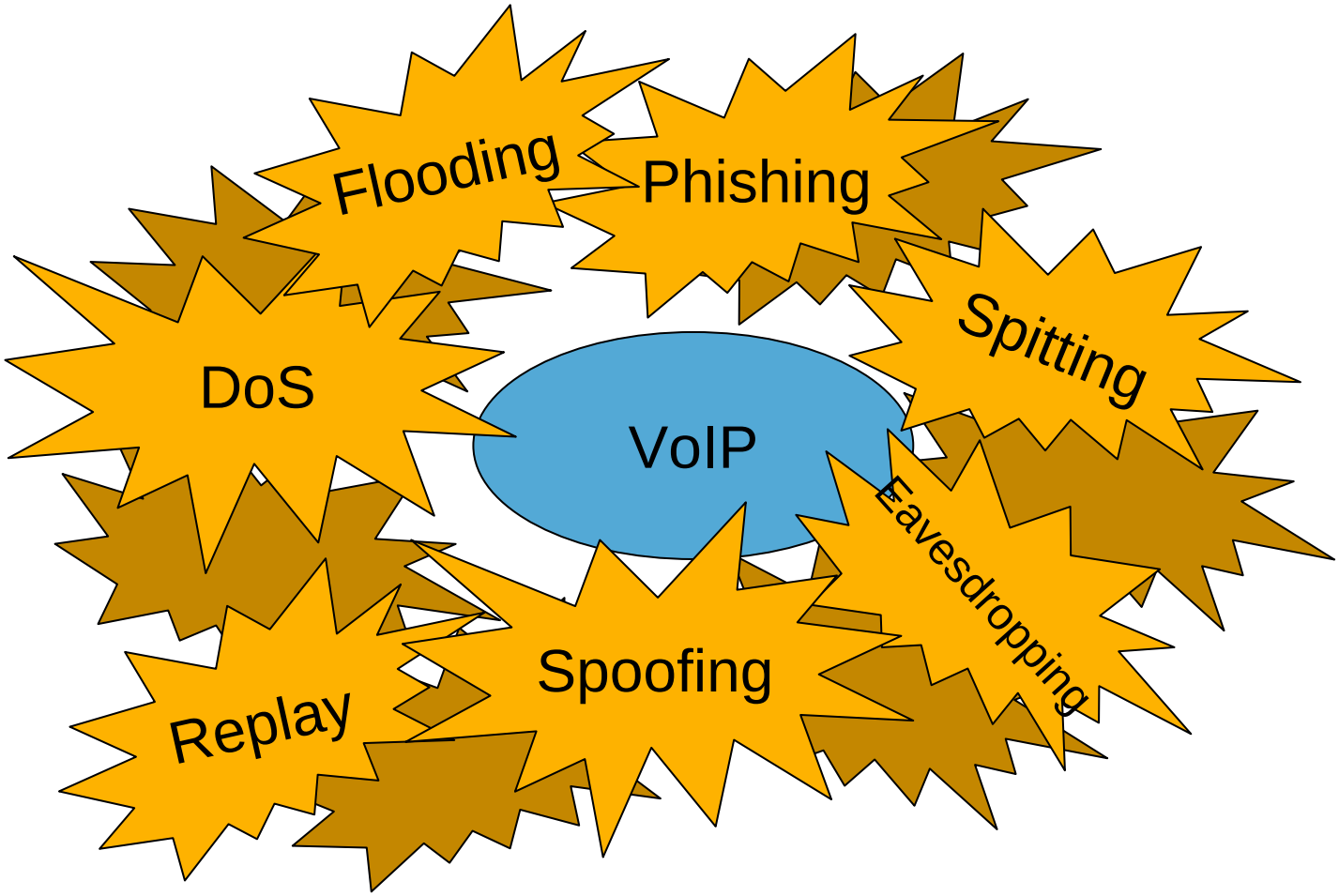
Security und VoIP

- Kapsch BusinessCom AG
- Systems Engineer bei techcom IT-solutions Consultant

- Entwicklung von IT-Sicherheitsstrategien, Planung und Umsetzung von IT-Security-Projekten

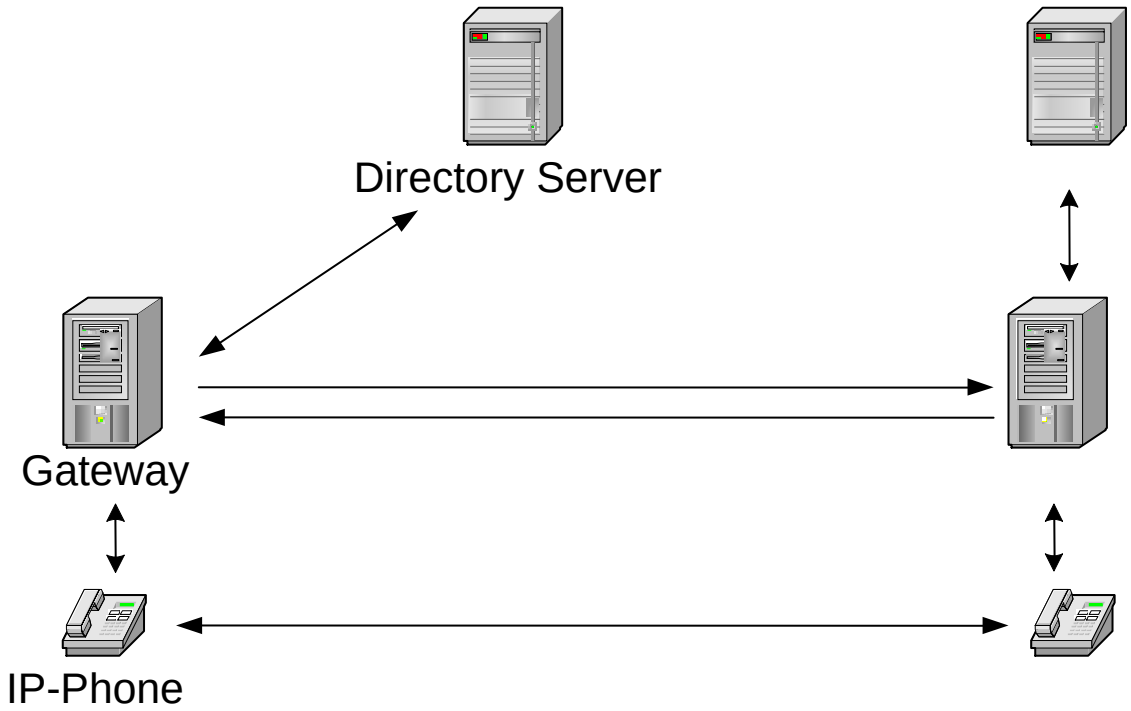
Security und VoIP

VoIP und die Bedrohungen



VoIP-Technik

VoIP-Systeme



Signalisierung

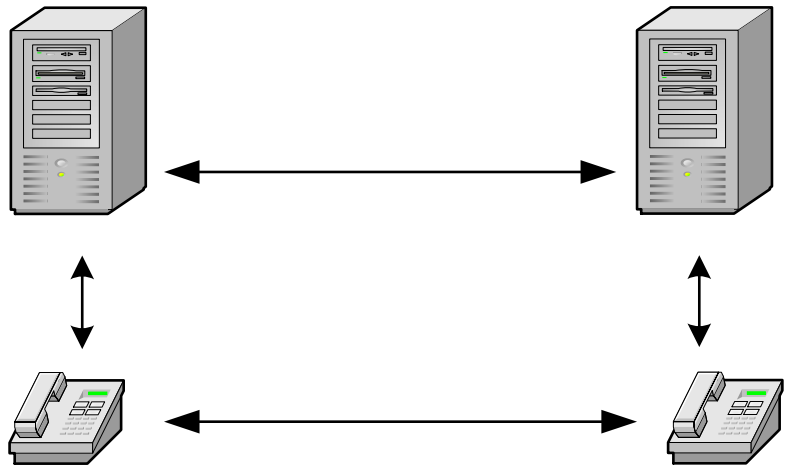
- H.323
  - Komplettes System für Multimedia (Audio und Video)
  - Angelehnt an ISDN, QSIG
  - Beschreibt Signalisierung und Medienübertragung
  - Komplexe Struktur
- SIP
  - Textbasierendes Signalisierungsprotokoll
  - Einfacher Aufbau, vergleichbar mit http
  - Adressierung ähnlich eMail-Adressen
  - Beliebige Daten übertragbar

RTP – Real-Time Transport Protocol

> Bestandteil der H.323 Spezifikation
> Sprach- und Videoübertragung
> End-to-End Protokoll
> UDP-Transport

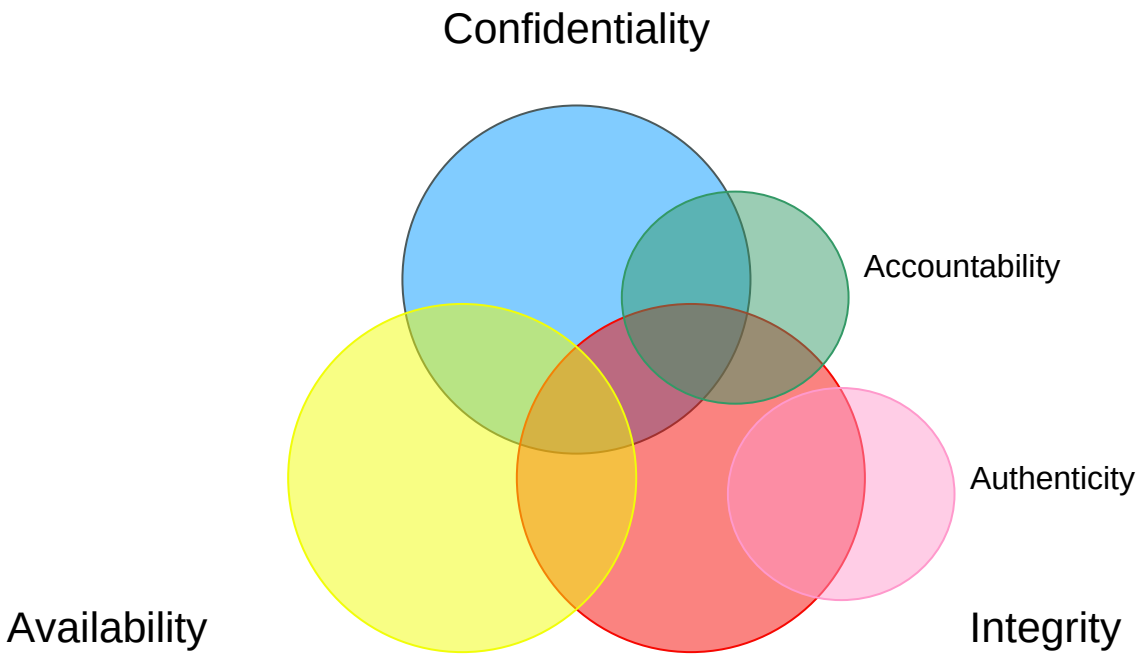
VoIP-Technik

> Unterschiede zur klassischen Telefonie
- Paket- statt sitzungsvermittelt
- Transportmedium nicht für QoS errichtet
- Gleiche Transportwege wie Datenströme
  - Auch jene von Fremdparteien (Internet)
- Direkter Kanal Endgerät-Endgerät

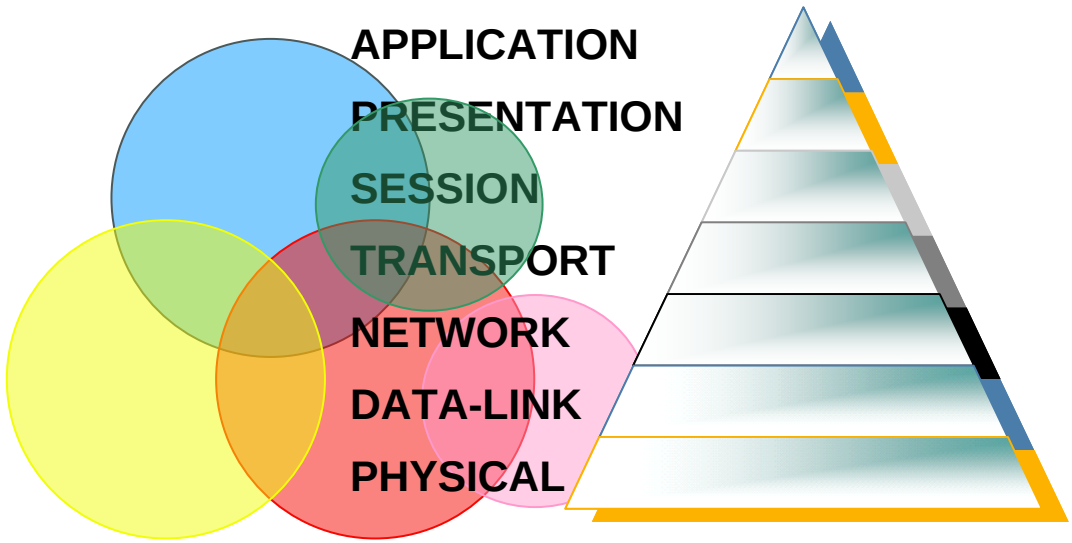


VoIP Bedrohungen

Security Evaluierung (C-I-A Triade)



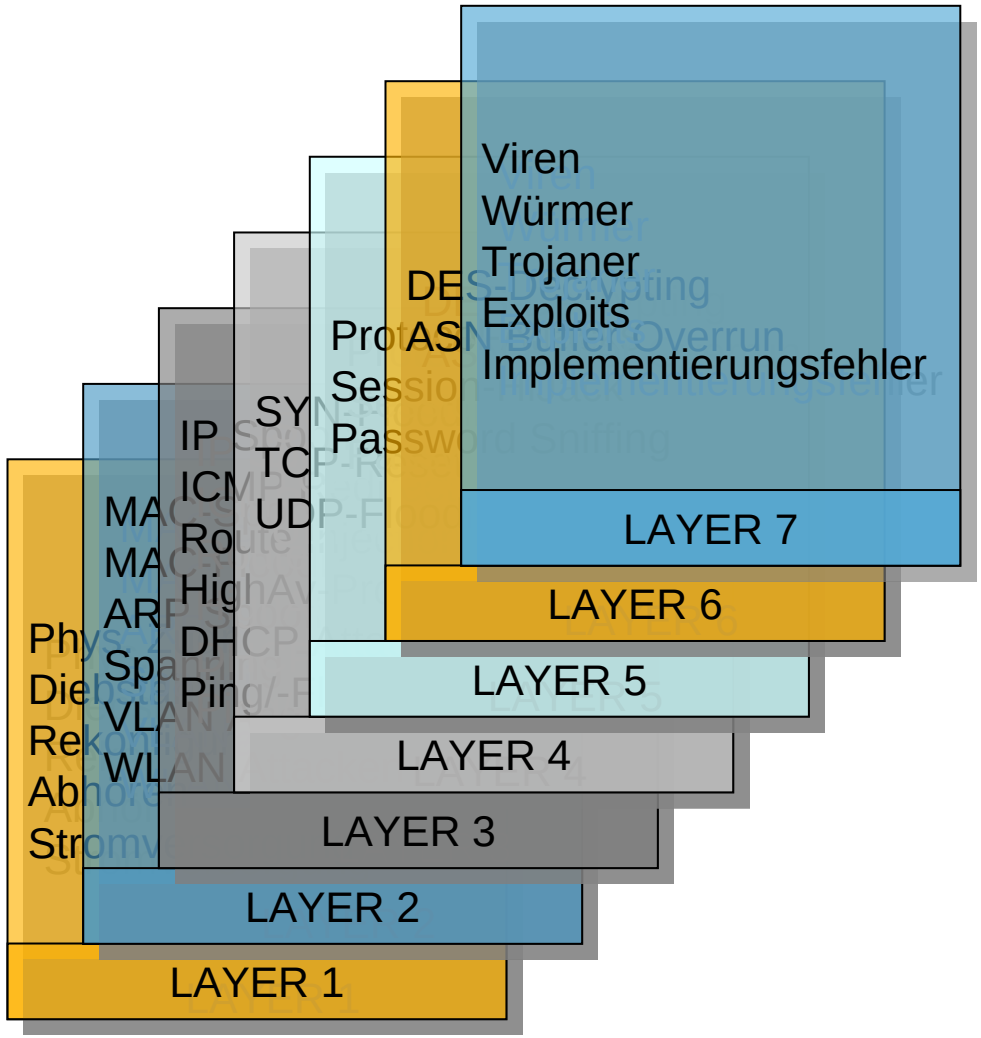
Security Evaluierung (C-I-A Triade)



Bedrohungen
C-I-A

Ebenen
OSI-Layer

Bedrohungen - Netzwerk



Bedrohungen der VoIP-Protokolle

> RTP
- Decodierung des Datenstroms
- Manipulation der Übertragung

> H.323
- VoIP-Address Spoofing
- Man-in-the-Middle Attacke
- Passwort-Authentifizierung in Klartext
- IP-Spoofing im Transport

> SIP
- Header-Manipulation
- Alle Angriffe wie bei H.323, nur einfacher (ASCII-formatiert)

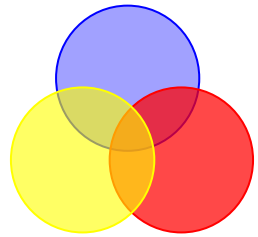
Bedrohungen der Infrastruktur – QoS

> QoS-Parameter
  - Packet Loss
  - Delay
  - Jitter

> QoS-Bedrohungen
  - Netzüberlasten
  - Konfigurationsfehler
  - DoS, DDoS
  - QoS-Attacken

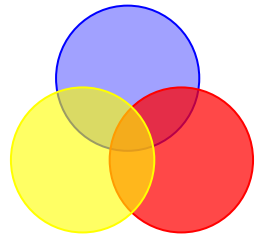
Sicherheitsmaßnahmen

Sicherheitsmaßnahmen – Layer 1

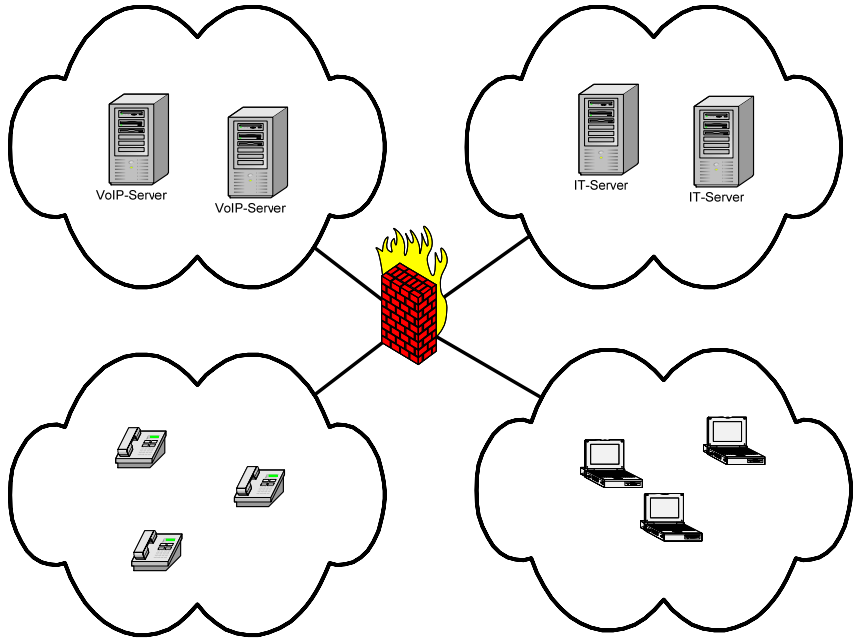


- Serverräume, Netzwerkverteiler
  - Zutrittsschutz und Überwachung
  - Environment (Feuer, Wasser, Klima)
- Verkabelungssysteme
  - Redundante Struktur
  - Zutritt zu Steigschächten
  - Abhörsichere Verkabelung
- Stromversorgung
  - Redundante Versorgung kritischer Systeme
  - Unterbrechungsfreie Stromversorgung
  - Power over Ethernet

Sicherheitsmaßnahmen – LAN

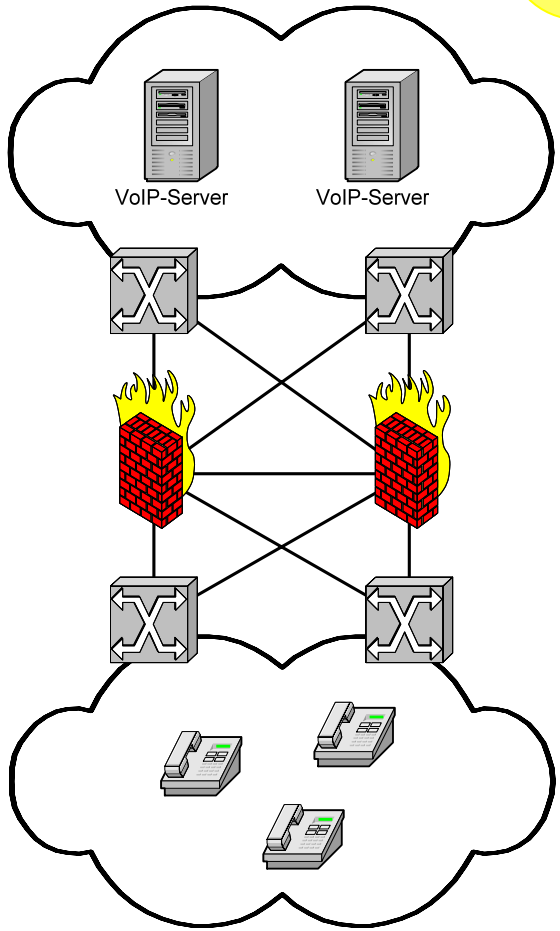


> VLAN-Struktur
- Getrennte Daten- und Voice-VLANs
- Firewalling zwischen VLANs
- CoS, QoS per VLAN
- Authentifizierung 802.1x
- Endpoint-Security

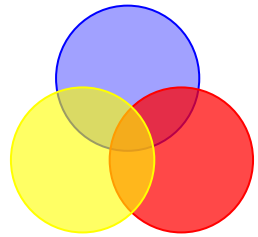


Sicherheitsmaßnahmen – LAN

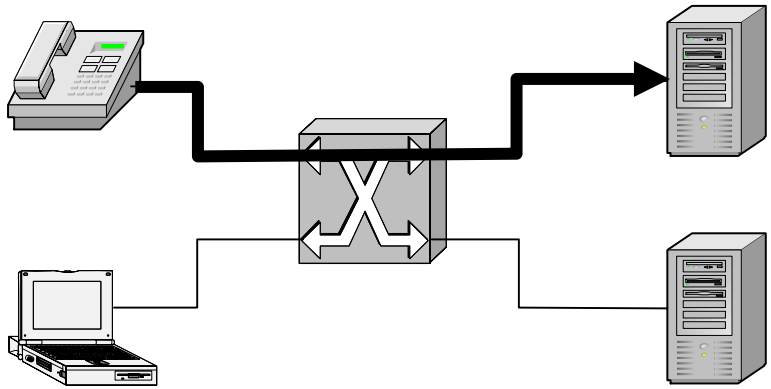
> Redundanz
- STP, RSTP
- VRRP, GLBP
- Firewall-Clustering
- Server-Clustering



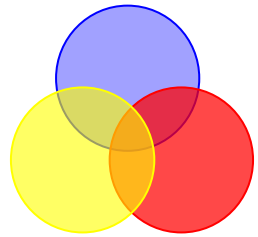
Sicherheitsmaßnahmen – LAN



> Quality of Service
  - CoS 802.1p
  - DiffServ
  - RSVP
  - Bandbreitenmanagement



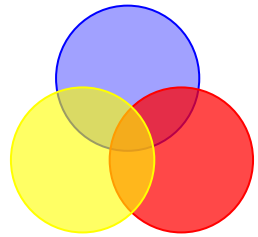
Sicherheitsmaßnahmen - LAN



- Firewalling
  - Firewall muss VoIP verstehen
    - UDP-Kommunikation
    - Dyn. Ports für Medienübertragung
  - Verbindungsmatrix
    - End-to-End
    - End-to System
    - System-to-System
  - QoS
- NIDS
  - Protocol Inspection
  - Angriffserkennung

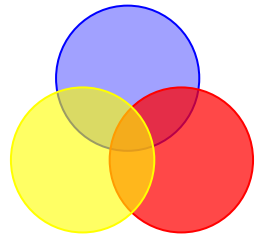
VoIP-Segment1	Gateway1	*	UDP sip	accept
VoIP-Segment1	VoIP-Segment2	*	?? sip_dynamic_port UDP sip_any	accept
Gateway1	Gateway2	*	TCP H323	accept
VoIP-Segment2	Gateway2	*	UDP H323_ras	accept

Sicherheitsmaßnahmen – WAN/Internet



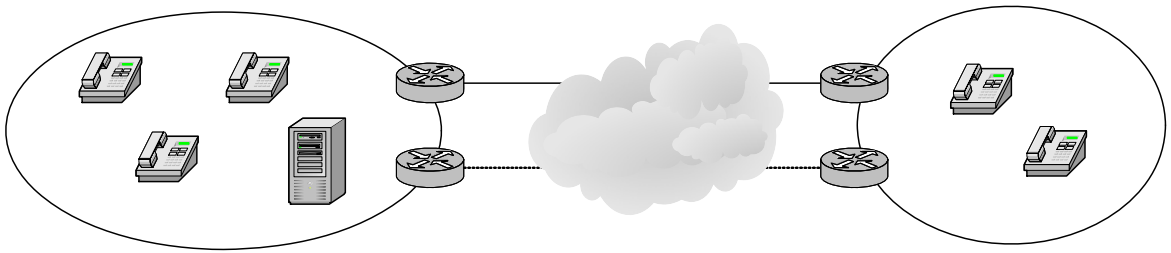
> Firewalling
- Intelligentes VoIP-NAT
  - Firewall erkennt und übersetzt IP im Datenfeld
  - Statisches und dynamisches NAT
- MidCom
  - Middlebox (NAT-Device) wird vom Gatekeeper gesteuert
- SBC
  - Session Border Controller wickelt Signalisierung und Medientansport ab

Sicherheitsmaßnahmen – WAN/Internet

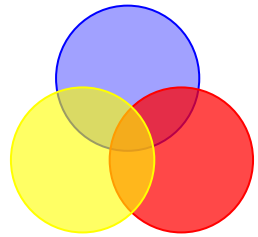


> QoS
- Priorisierung am Edge-Router
- QoS-fähiges WAN (z.B. MPLS)
- Dienstgüte im WAN
  - Packet Loss, Delay, Jitter
- Überlastbehandlung

> Redundanz
- Multi-Peering
- Backup-Routen

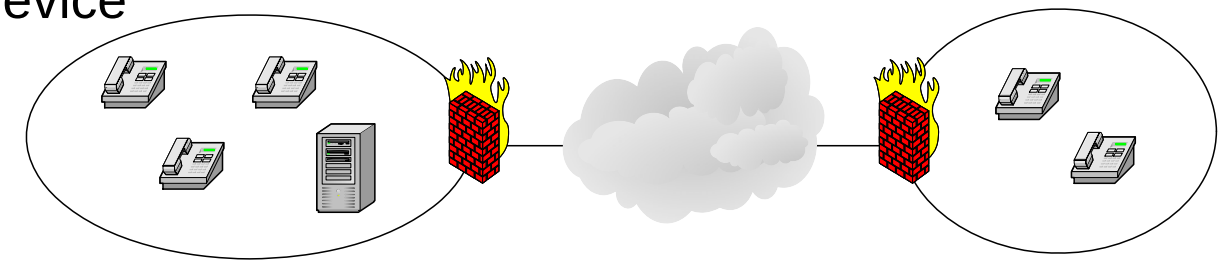


Sicherheitsmaßnahmen – WAN/Internet

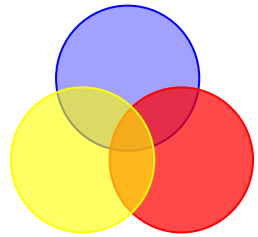


> VPN
- Site-to-Site VPN
  - Encryption/Authentication
  - Ausfallsicherheit
- Client-VPN
  - Softphone

- QoS im VPN
  - VoIP-Header wird mitverschlüsselt
  - QoS vor VPN
  - QoS im VPN-Device
  - IPv6

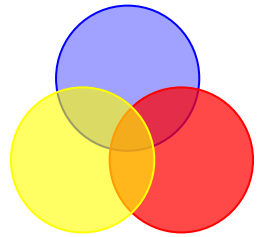


Sicherheitsmaßnahmen – Systeme



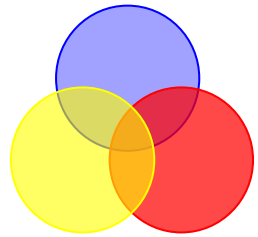
- Betriebssystem
  - Admin-Zugänge sichern
    - ssh, https
    - Management-VLAN
  - OS-Hardening
    - Minimalsystem
    - Security-Patches
  - Backup
    - Clustering
    - Datensicherung
- HIDS

Sicherheitsmaßnahmen – Protokolle



> Sichere Signalisierung in H.323 (H.235v3)
- Einsatz kryptografischer Verfahren
  - IPSec oder TLS
- Media Antispam
  - Message Authentication mit SHA1-96
- Hop-by-Hop Authentication
  - Benutzer, Signalisierung
- Direkte Signalisierung
  - Key-Exchange zwischen Endgeräten
  - Gatekeeper wird zum Key Distribution Center
- SRTP

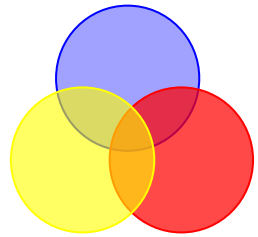
Sicherheitsmaßnahmen – Protokolle



> Sichere Signalisierung in SIP (SIP 2.0)

- HTTP Digest Authentication
  - Hop-to-Hop
  - Auf allen SIP-Komponenten implementiert
  - Keine Integrität/Authentizität der Gesamtnachricht
    - Ergänzung z.B. mit TLS
- S/MIME
  - SIP-Nachricht ähnelt E-Mail
  - SDP-Body signiert und ggf. verschlüsselt
  - Sicherer Key-Exchange z.B. für SRTP
- SIP über TLS
  - Hop-to-Hop
  - UDP->TCP
- SIP über IPSec

Sicherheitsmaßnahmen – Protokolle



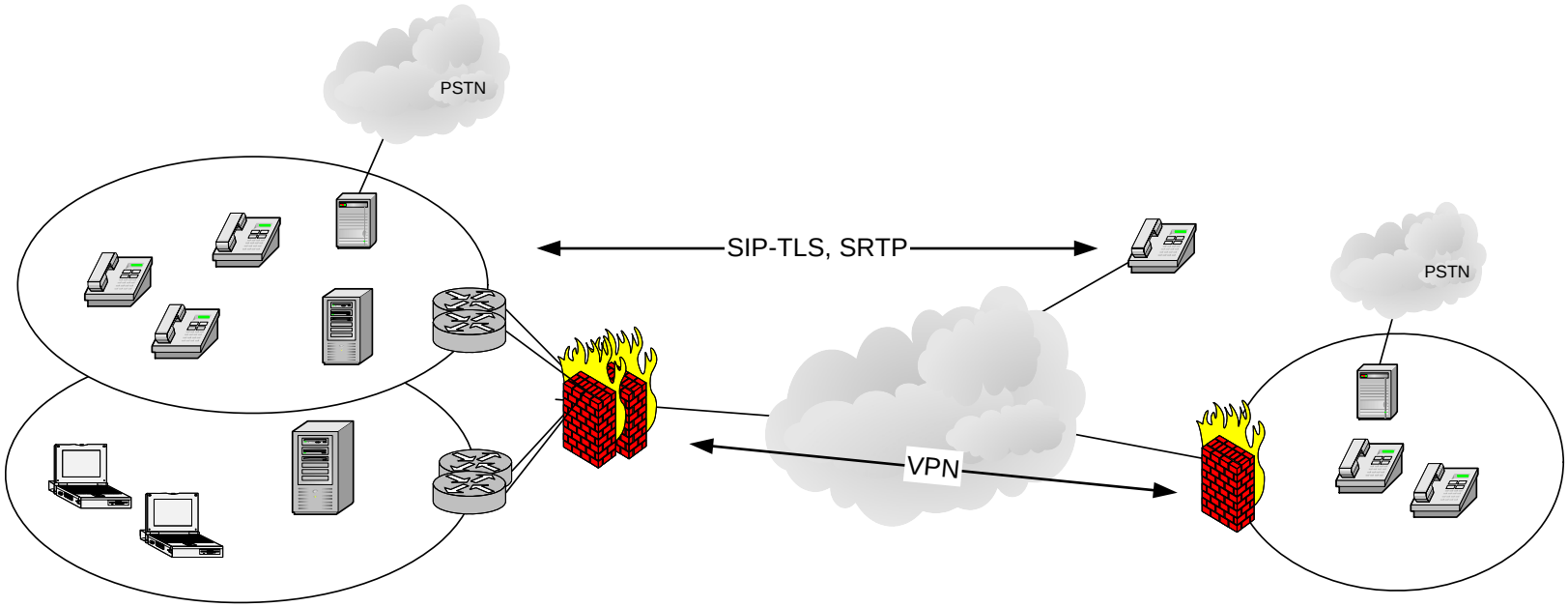
> Sichere Medienübertragung SRTP
  - Verschlüsselung, Authentifizierung
    - AES, SHA-1
  - Replay-Schutz
  - Key-Management MIKEY

> IPSec
  - Für VoIP nur bedingt geeignet, da
    - QoS-Problem
    - Timing des Key-Exchanges
    - ESP-Overhead
    - CPU-bedingte Latenz im Endgerät

Welche Vorgehensweise?

Security-Konzept

> Kombination von Security-Maßnahmen
- Geeignete Techniken einsetzen
- Synergien nutzen



VoIP-Security am Markt

> VoIP-Systeme
  - Vermehrt Einsatz von SRTP, SIP-TLS

> LAN-Komponenten
  - QoS Standards
  - 802.1x, Endpoint Security

> VoIP-Firewalls
  - „verstehen“ VoIP-Protokollen
  - Integriertes QoS

> Proprietäre Lösungen
  - Secure SCCP

Ihre Entscheidung

> Security ist ein Entscheidungskriterium
  - Funktionalität und Security als Gesamtkonzept
  - VoIP wird mehr und mehr Plug-and-Play, VoIP-Security nicht
  - Nehmen Sie den Lieferanten in die Pflicht

> Nutzen Sie Ihre bestehenden IT-Systeme
  - Viele Sicherheitsfeatures sind bereits integriert (Switches)
    - Sie müssen oft nur aktiviert werden

> Erstellen Sie ein Sicherheitskonzept
  - Überlegen Sie die für Ihr System geeigneten Maßnahmen
  - Beachten Sie C-I-A
  - Beachten Sie die OSI-Layer

Zukunft

- Komplexität
  - IP-Phones leisten immer mehr
    - Kalender, ToDo-Listen, Medienwiedergabe, Browser
- Erweiterbarkeit
  - Mobile Code am Phone
    - Java, API´s
- Connectivity
  - WLAN-Hotspots
  - Mobile SoftPhone

- Risikobewertung
  - Change Management

Conclusio

> VoIP-Security Standards und Techniken existieren
- Umsetzung in den Systemen schreitet voran
- Implementierung teilweise noch mangelhaft
- Überarbeitung der Standards notwendig

> IT-Infrastruktur kann Lücken schließen
- Viele Techniken der IT-Security anwendbar
- QoS als wesentliches Unterscheidungsmerkmal

> Einsatz von VoIP dem Stand der (Security-)Technik anpassen

Vielen Dank für Ihre Aufmerksamkeit

Enabling effective real time business