RUS CERT

Sicherheit und Sprach-dienste (VoIP)

8. Tagung der DFN-Nutzergruppe Hochschulverwaltung

Halle – 2007-05-08

Oliver Göbel

http://CERT.Uni-Stuttgart.DE/

Das RUS-CERT

Stabsstelle DV-Sicherheit der Universität Stuttgart

Computer Emergency Response Team

- Gründung 1998
- Stabsstelle der Kanzlerin der Universität Stuttgart
- Zuständig für die DV-Sicherheit an der Universität Stuttgart
- Mitglied in nationalen (CV), europäischen (TI/TF-CSIRT) und internationalen Verbänden (FIRST)
- F&E in Bereichen Standardisierung und Technologie
- Mit-/Veranstalter regelmäßiger Konferenzen (Sept: IMF 2007)

VoIP an der Universität Stuttgart

- 2006 Inbetriebnahme einer VoIP-Anlage
- Ersetzt klassische Zweidraht-Anlage
- Benutzt das vorhandene Datennetz der Uni
- RUS-CERT hat Projekt im Bereich Sicherheit begleitet und Anforderungen sowie Implementierung festgelegt

Komponenten einer VoIP-Anlage

- Vermittlungsrechner (oft auch ‘Callserver‘)
- Systeme für die Abrechnung
- Telefone
- Systeme für Mehrwertdienste

VoIP – Prinzip der Netztopologie

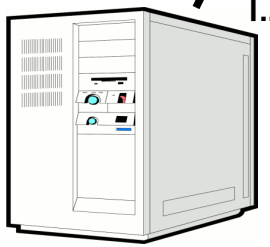
1.2.3.4

1.2.12.220

IP-Netzwerk

1.2.189.7

1.2.3.5



1.2.200.1

Callserver

Grundsätzlich sind alle Komponenten einer VoIP-Anlage reguläre Netzteilnehmer

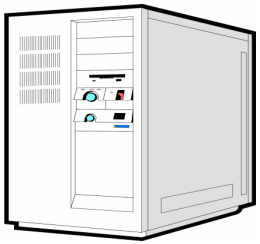
VoIP - Funktionsprinzip

A ...83678

B

1.2.3.4

1.2.3.5



Callserver

1. Benutzer A wählt Nummer des Telefons B

VoIP - Funktionsprinzip

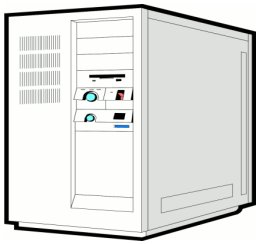
A ...83678

B

1.2.3.4

IP?

1.2.3.5



Callserver

1. Benutzer A wählt Nummer des Telefons B
2. A fragt Server nach IP-Adresse von 83678

VoIP - Funktionsprinzip

A

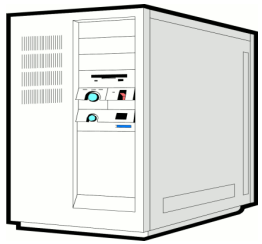
B

1.2.3.4

IP?

1.2.3.5

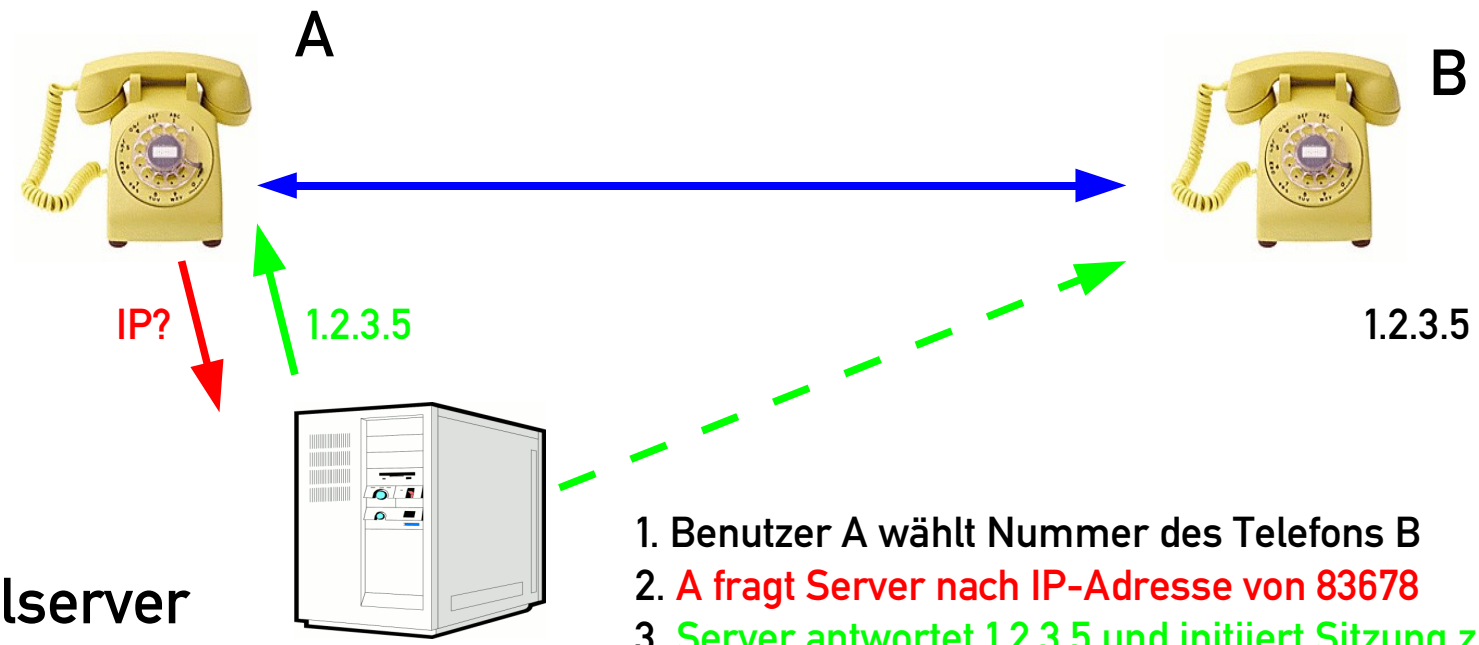
1.2.3.5



Callserver

1. Benutzer A wählt Nummer des Telefons B
2. A fragt Server nach IP-Adresse von 83678
3. Server antwortet 1.2.3.5 und initiiert Sitzung zu B

VoIP - Funktionsprinzip



1. Benutzer A wählt Nummer des Telefons B
2. A fragt Server nach IP-Adresse von 83678
3. Server antwortet 1.2.3.5 und initiiert Sitzung zu B
4. 1.2.3.4 baut Sprachverbindung mit 1.2.3.5 auf

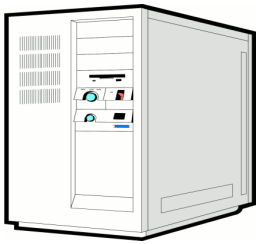
VoIP - Funktionsprinzip

A

B

1.2.3.4

1.2.3.5



Callserver

Sprachverbindung zwischen 1.2.3.4 und 1.2.3.5 besteht ohne weiteres Zutun weiterer Komponenten der Anlage

VoIP und Sicherheit

- ...sind nicht orthogonal, auch wenn viele Implementierungen das so erscheinen lassen
- Mitbenutzung eines i.d.R. vorhandenen Datennetzes erzeugt Implikationen auf die Sicherheit
  - → des zu implementierenden VoIP-Systems
  - → des vorhandenen Datennetzes
- Beide Aspekte sind unbedingt zu beachten! Insbesondere in einer Hochschulumgebung, die i.A. sehr offen gestaltet ist und vergleichsweise wenig Sicherheitsmaßnahmen implementiert.

Implikationen für das Telefonie-System

- Sicherheit des Datennetzes vererbt sich auf die VoIP-Infrastruktur
  - ➔ Anforderungen einer Telefonanlage sind mit den Anforderungen der IT und den Fähigkeiten des Netzes abzugleichen, Schwachpunkte sind zu identifizieren
- Schwachstellen und Angriffe auf die IT-Infrastruktur betreffen nun auch die Telefonie
- Angriffsreichweite wird durch vernetzte IT drastisch erhöht

Implikationen für das Datennetz

- Zahlreiche neue Systeme werden installiert
- neue Protokolle kommen hinzu
- Anforderungen der Telefonie schwächen u.U. bestehende Sicherheitsmaßnahmen

➔ neue und/oder unbekannte Angriffsmöglichkeiten entstehen für das vorhandene Netz

VoIP - Sicherheitsanforderungen

- Vertraulichkeit
  - Sprachkommunikation
  - Verkehrsdaten (Gesprächsranddaten)
- Authentizität
  - Teilnehmer bzw. deren techn. Repräsentanten
  - Verkehrsdaten
- Integrität
  - Verkehrsdaten
  - System
- Verfügbarkeit (Robustheit gegenüber Angriffen)

Was bietet das Netz an Sicherheit?

- Integrität – Systeme und Daten sollen nicht kompromittiert werden: wird durch Maßnahmen zur Systemsicherheit und Verschlüsselung erreicht
- Authentizität der teilnehmenden Parteien nur mit zusätzlichen Technologien sicherstellbar
- Vertraulichkeit der Daten i.A. entweder auf Anwendungsebene oder mit Zusatztechnik realisierbar
- Robustheit gegenüber Ausfall oder Betriebseinschränkung bei Angriffen: Patches, Zusatztechnologie

→ Übliche Netztechnologie bietet relativ wenig Sicherheit

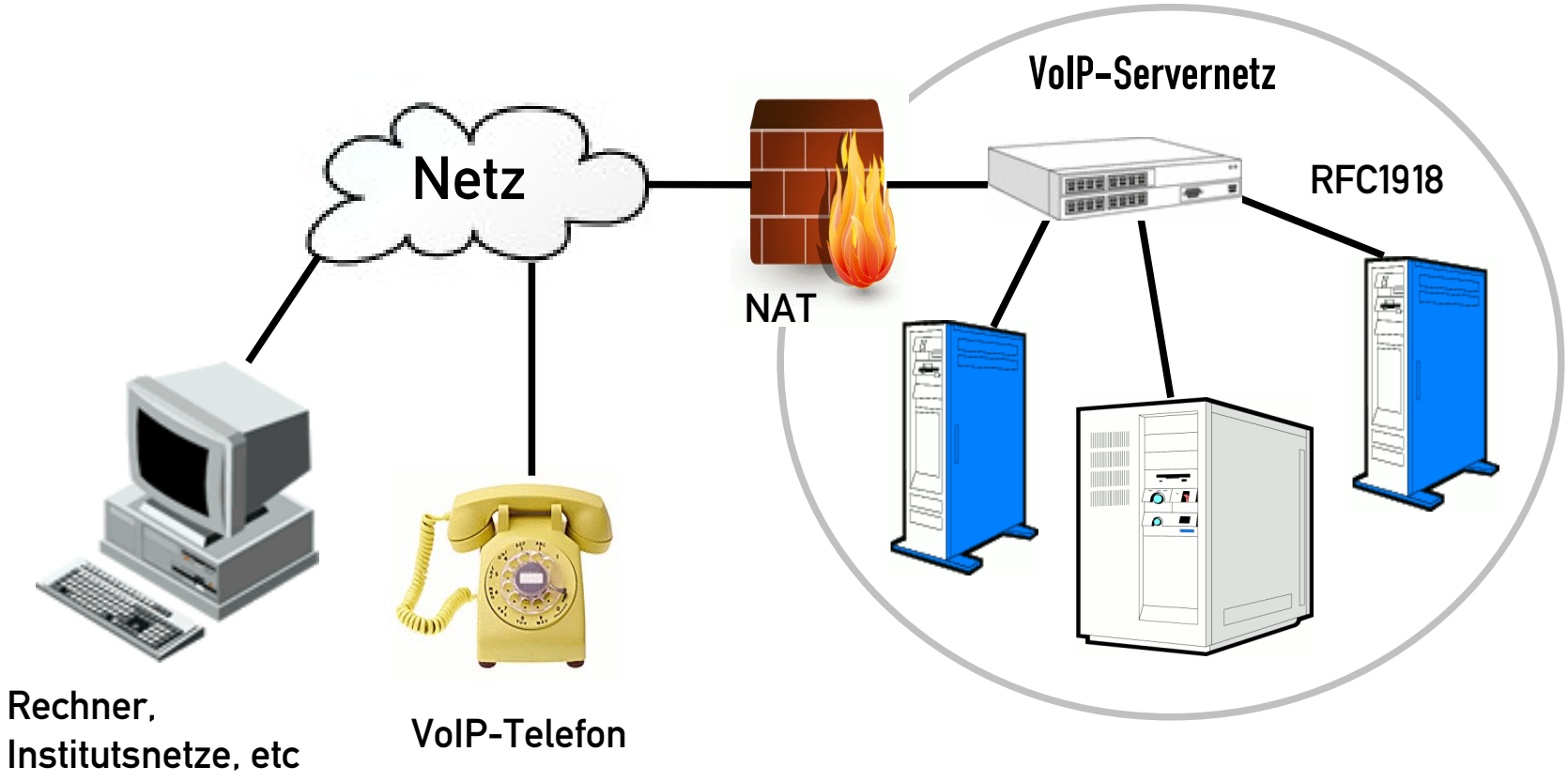
VoIP im Datennetz

- Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit[1)] in fast allen Datennetzen nur mit zusätzlichen Technologien implementierbar ‘vererbtes‘ Risiko aber auch so nicht zu beseitigen
- ➔ Weitgehende Trennung von Daten- und Voice-Netz sinnvoll, bzw. erforderlich
  - physikalische Trennung – kann im Gesamtsystem nicht ohne Verlust kapitaler Einsparungseffekte vorgenommen werden
  - ‘virtuelle‘ Trennung durch VLANs und ggf. weitere Technologien

VoIP-Servernetz

- Die zentralen Komponenten einer VoIP-Anlage können relativ leicht vom Rest des Netzes separiert werden:
  - Müssen nur untereinander und nach ‘außen‘ mittels genau definierter Protokolle kommunizieren (i.W. die Mehrwertdiensteserver)
  - Größte Gruppe externer, regelmäßiger Kommunikationspartner sind die Telefone
- Schaffung eines abgeschotteten VoIP-Servernetzes mittels Firewalls und der Nutzung privater IP-Adressen (nach RFC1918) effektiv möglich und sinnvoll

VoIP-Servernetz



Voice-Netz

- Die Telefone, die ‘im Feld‘ stehen müssen mit anderer Technologie vom Datennetz getrennt werden.
- VLANs (IEEE 802.1q) ermöglichen, Netze virtuell zu trennen und auf den Netzkomponenten verschieden zu behandeln
- Für VLANs können Ressourcen reserviert werden (IEEE 802.1p) und so die (Mindest-)Qualität z.B. eines Dienstes sichergestellt werden (Verfügbarkeit)

VLAN-Technologie

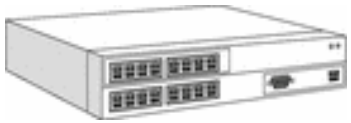
- Virtual Local Area Network-Technologie basiert auf OSI-Layer 2
- Trennung des Verkehrs erfolgt durch Kennzeichnung ('tagging') der Pakete
  - → Zugriffsschutz wird nur durch teilnehmende Systeme gewährleistet
  - → deren Kompromittierung kompromittiert auch die Trennung
- Aber: verteilte Administration stellt ein Problem dar

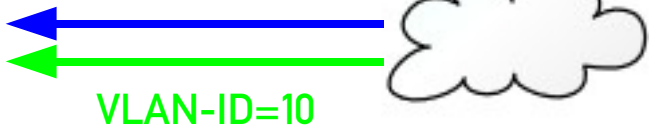
VLAN (IEEE 802.1Q)

Gerät A

00:12:3F:E6:D2:E7

Switch





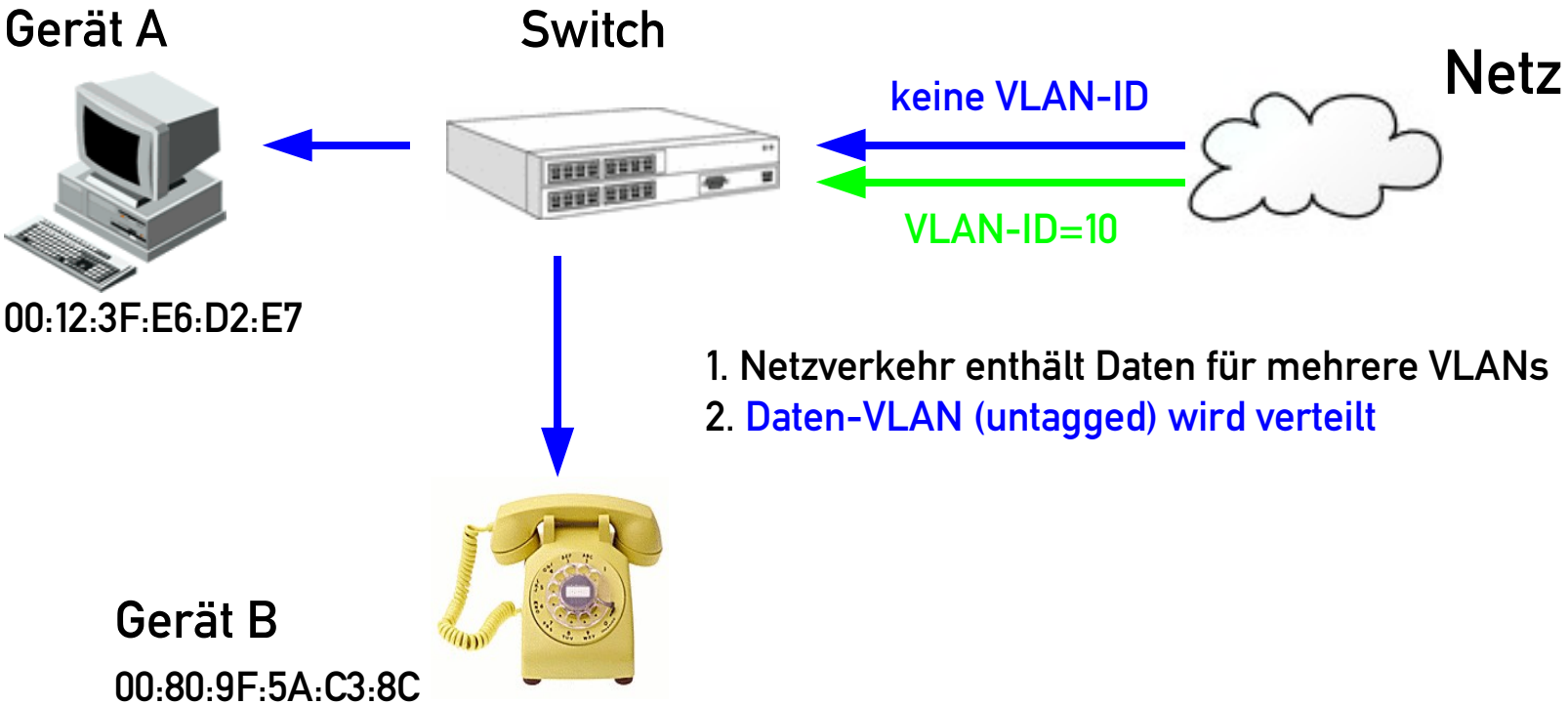
Netz

1. Netzverkehr enthält Daten für mehrere VLANs

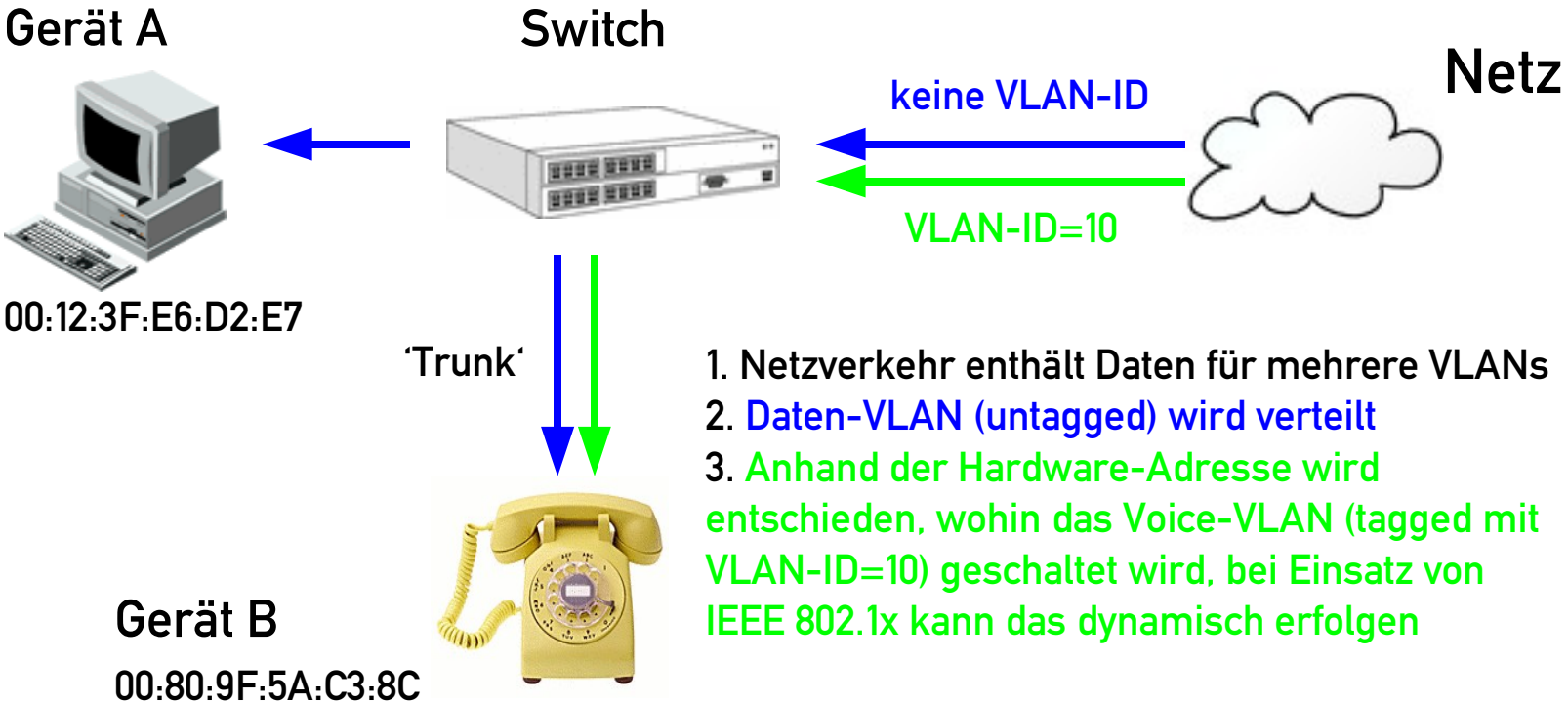
Gerät B

00:80:9F:5A:C3:8C

VLAN (IEEE 802.1Q)



VLAN (IEEE 802.1Q)



1. Netzverkehr enthält Daten für mehrere VLANs
2. Daten-VLAN (untagged) wird verteilt
3. Anhand der Hardware-Adresse wird entschieden, wohin das Voice-VLAN (tagged mit VLAN-ID=10) geschaltet wird, bei Einsatz von IEEE 802.1x kann das dynamisch erfolgen

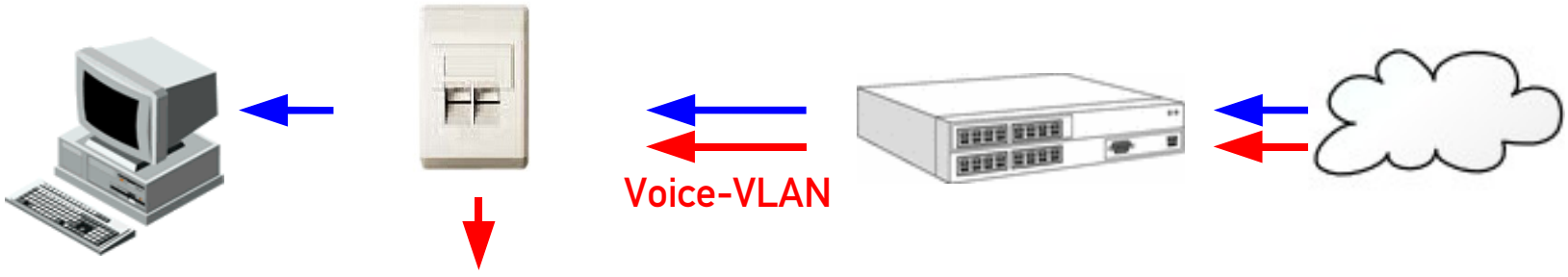
Probleme bei VLANs

- Sicherheit der übertragenen Daten basiert nur auf der Sicherheit der Netzwerkinfrastruktur
  - → Erfolgreicher Angriff auf den Switch kompromittiert auch die Daten des Voice-VLANs
- Hardware-Adressen fälschbar
  - → selbst bei Einsatz von Basis-IEEE 802.1x kann ein Switch dazu veranlasst werden, das Voice-VLAN auf einen beliebigen Port zu schalten

Besondere Probleme: Daisy-Chaining

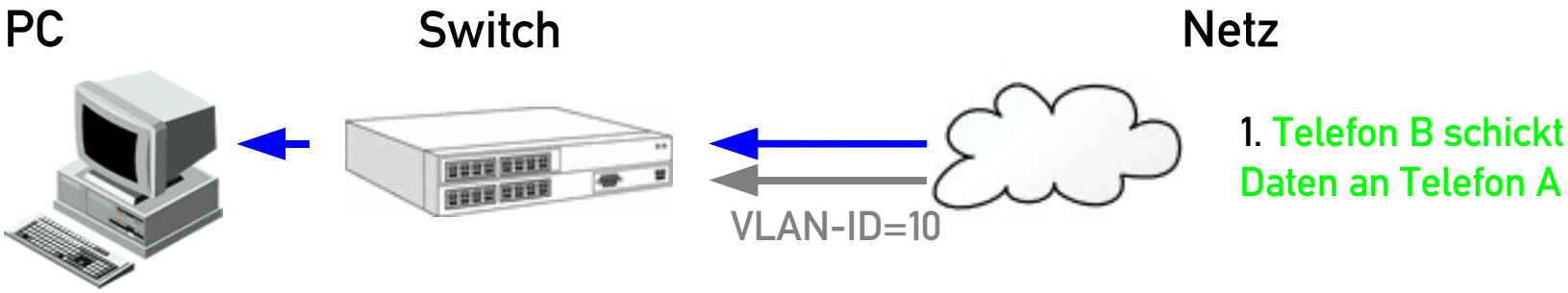
- Keine Netzdosen/Verkabelung exklusiv für VoIP
  - ➔ Dosen für PCs vorhanden, jedoch nicht für Telefone
  - ➔ Mehrfachbelegung durch ‘daisy-chaining‘: Netzwerkdose-Telefon-Rechnersystem
- Probleme:
  - Telefone müssen Voice-VLAN korrekt filtern andern-falls stellen sie ‘Zugang‘ zum Voice-VLAN bereit
  - Telefone ‘sehen‘ sämtlichen Verkehr

Daisy-Chaining

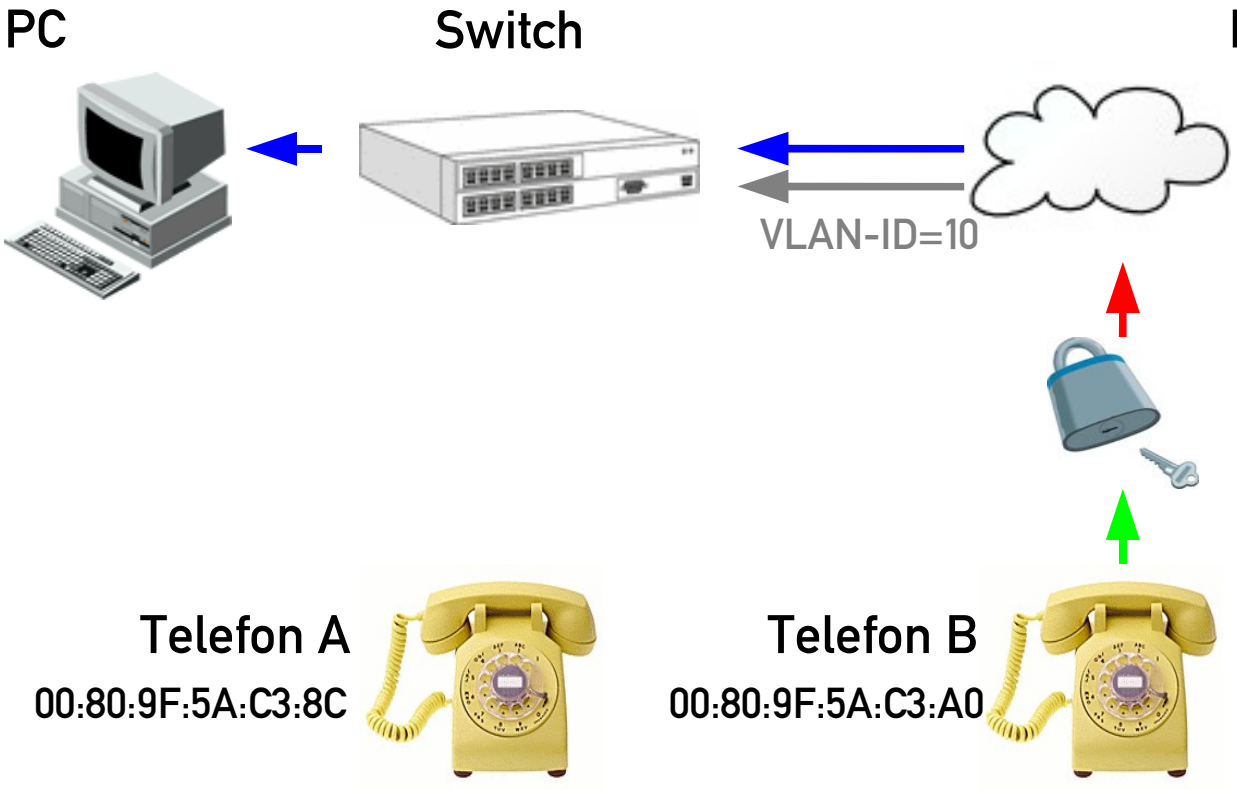


Um Daisy-Chaining zu ermöglichen, sind bei vielen VoIP-Telefonen Mini-Switches eingebaut, die über die Netzwerkdose den Trunk mit Daten- und Voice-VLAN empfangen, das Voice-VLAN an das Telefon schicken und das Daten-VLAN an den angeschlossenen Rechner.

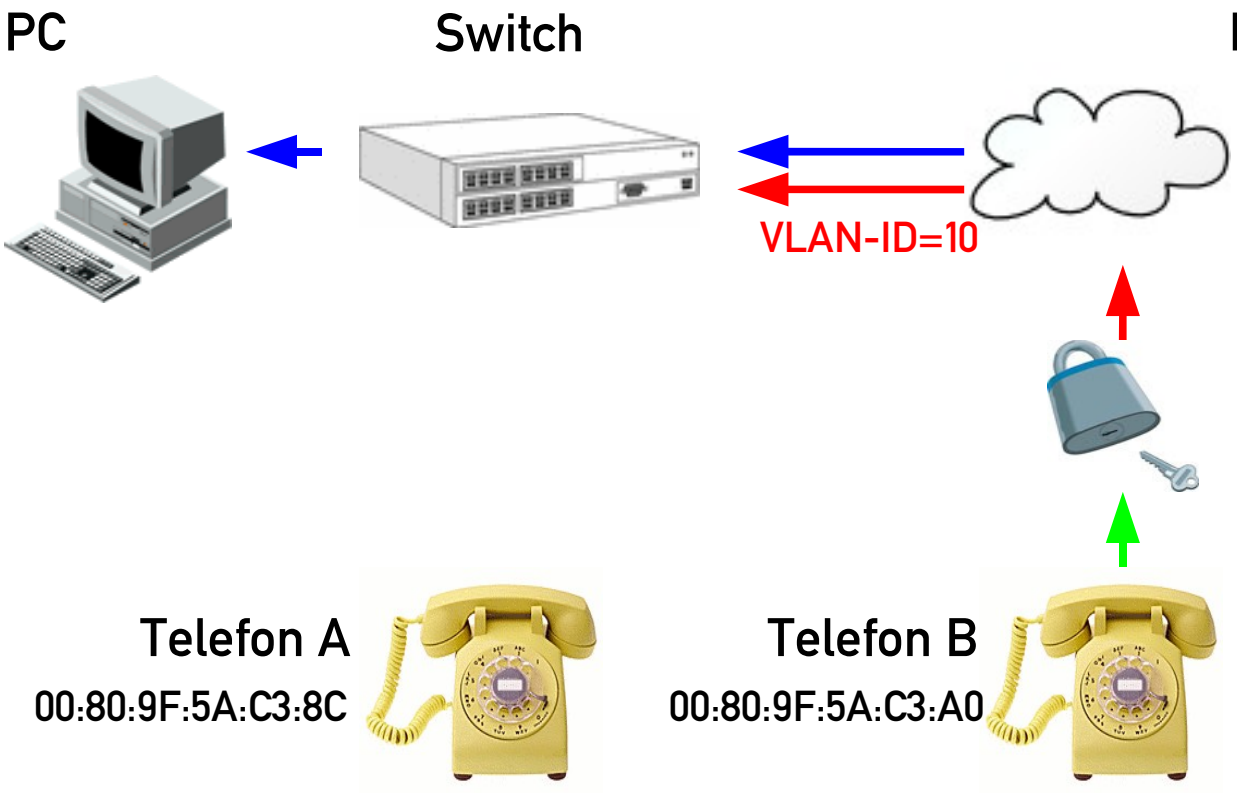
Lösung: Verschlüsselung



Lösung: Verschlüsselung

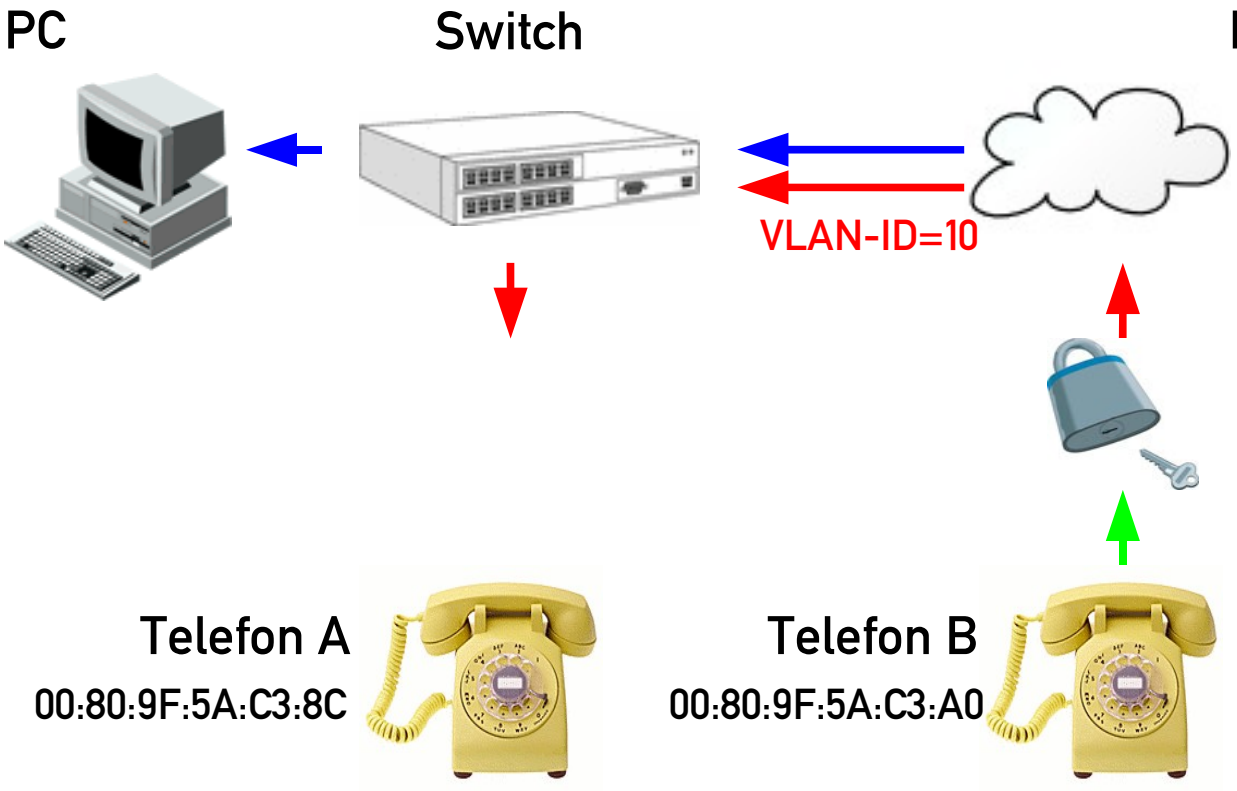


Lösung: Verschlüsselung



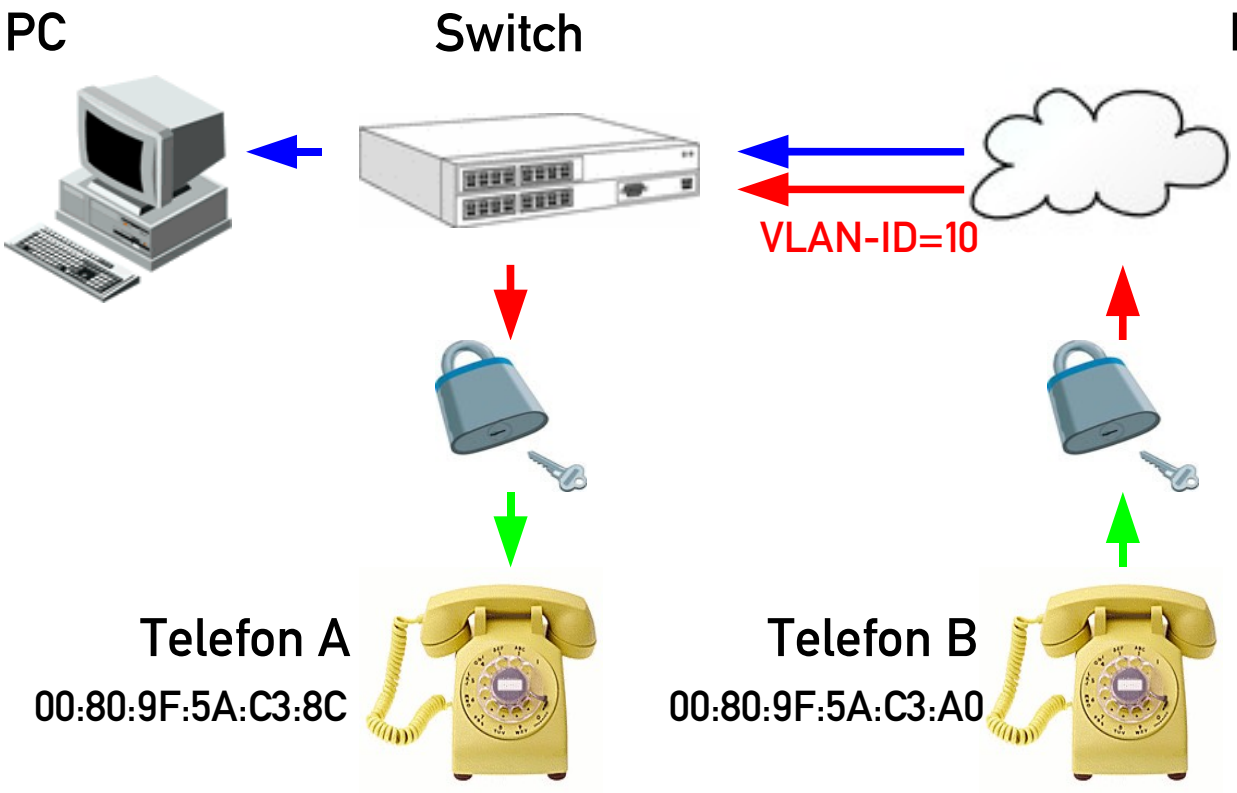
1. Telefon B schickt Daten an Telefon A
2. Telefon B verschlüsselt die Daten und fügt VLAN-ID=10 hinzu
3. Die Daten werden im VLAN übertragen

Lösung: Verschlüsselung



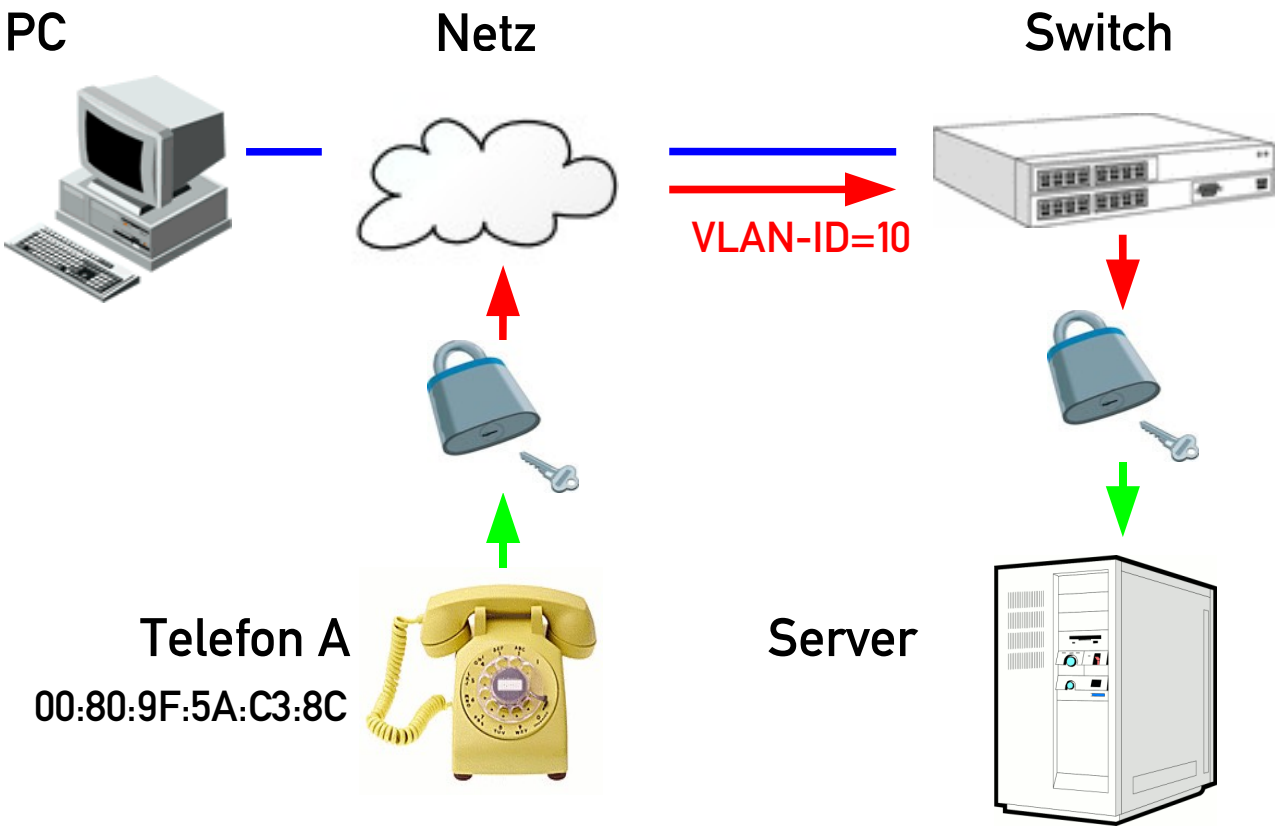
1. Telefon B schickt Daten an Telefon A
2. Telefon B verschlüsselt die Daten und fügt VLAN-ID=10 hinzu
3. Die Daten werden im VLAN übertragen
4. Switch leitet Daten an Telefon weiter

Lösung: Verschlüsselung



1. Telefon B schickt Daten an Telefon A
2. Telefon B verschlüsselt die Daten und fügt VLAN-ID=10 hinzu
3. Die Daten werden im VLAN übertragen
4. Switch leitet Daten an Telefon weiter
5. Telefon A entschlüsselt Daten

Analog für Signalisierung



Oliver Göbel

Kryptographie: Fazit

- Der Einsatz kryptographischer Technologien zur Absicherung der Signalisierung sowie der Sprachdaten in einer VoIP-Anlage kann tatsächlich eine effektive Trennung des Sprach- und Datennetzes implementieren und so die Anforderungen an die Sicherheit erfüllen.
- Auch die Hersteller haben dies z.T. erkannt und beginnen nun, solche Lösungen anzubieten.

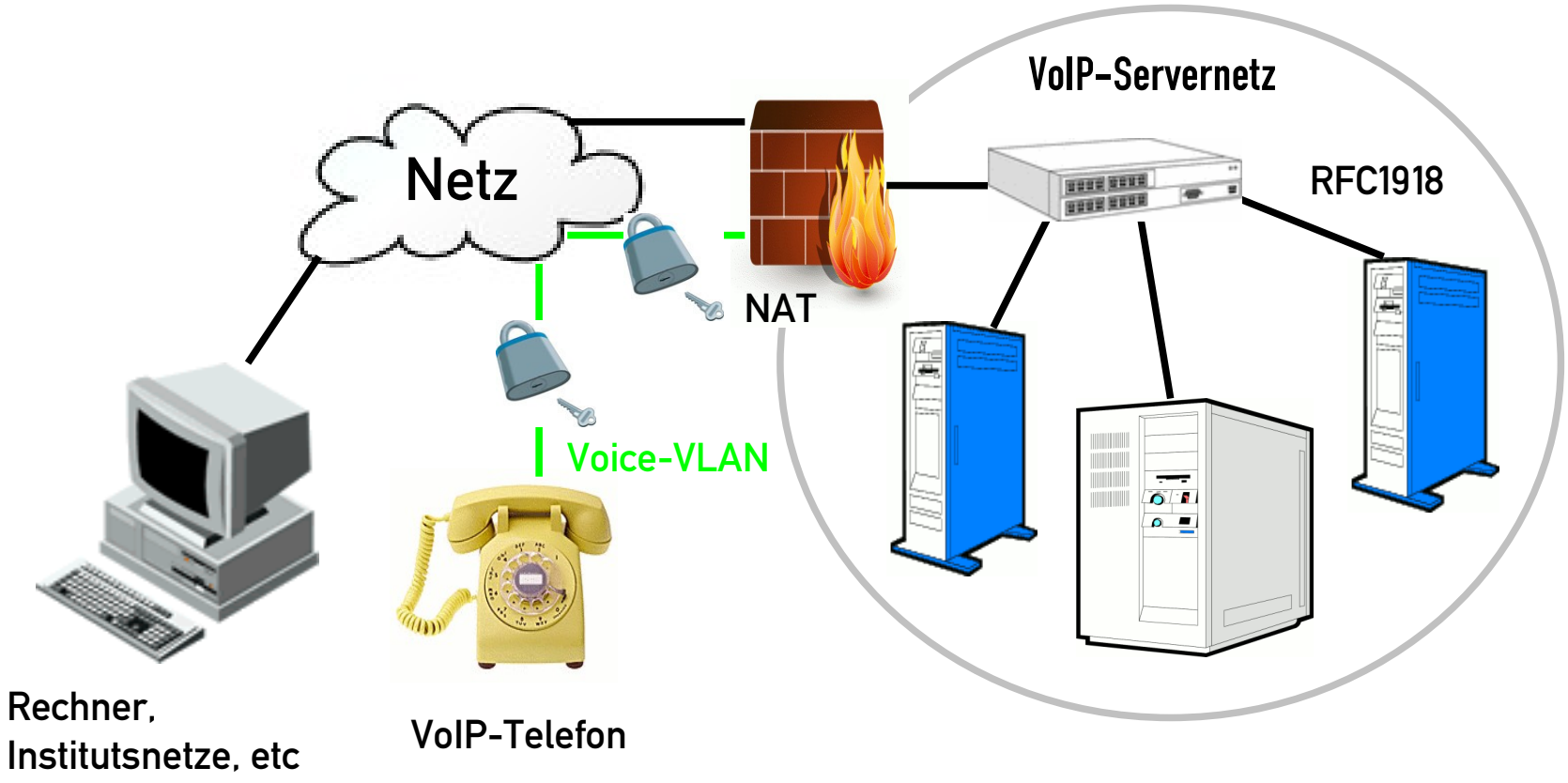
Besonderes Problem: Softphones

- Softphones sind Anwendungen, die auf normalen Rechnersystemen laufen und Telefonfunktionalität bereitstellen. Dazu benötigen sie Zugriff auf das VoIP-Netz
- → SP heben die Trennung der Netze effektiv auf
- → Dadurch bedrohen Angriffe auf das normale Datennetz das VoIP-System, insbesondere Malware stellt eine ernste Bedrohung dar.
- → Einzig sinnvolle Konsequenz: Softphones dürfen nicht äquivalent zu Hardphones eingesetzt werden

Zusammenfassung

- Die Einführung eines VoIP-Systems in ein vorhandenes Datennetz birgt neue Risiken sowohl für das Telefoniesystem als auch für das Datennetz.
- Eine Trennung des VoIP-Netzes vom Datennetz erhöht die Sicherheit effektiv.
- Die zentralen Komponenten können relativ leicht in einem zentralen Servernetz vom restlichen Netz abgeschottet werden.
- Zur Separierung der Telefone soll ein VLAN sowie starke Kryptographie eingesetzt werden.

VoIP-Servernetz



Vielen Dank

Haben Sie Fragen?