# Security für VoIP

## Verschlüsselung, Authentisierung und Firewalls

**Während bei der traditionellen Telefonie das Thema Sicherheit eine eher untergeordnete Bedeutung spielte, kann man sich diesem bei der Integration in die IP-Welt nicht mehr entziehen, ohne grob fahrlässig zu handeln. Wer seine VoIP-Installation adäquat schützen will, sollte sowohl mit den drohenden Gefahren als auch den Gegenmaßnahmen vertraut sein. Der Kurs analysiert systematisch Angriffspunkte von VoIP und stellt die zur Verfügung stehenden Schutzmaßnahmen auf Netzwerk- und Applikationsebene dar. Letztere werden dann auf der Basis der unterschiedlichen VoIP-Architekturen gegeneinander abgewogen. Die Teilnehmer lernen, wie sie in späteren eigenen Projekten für eine angemessene Sicherheit von VoIP sorgen können.**

**Kursinhalt**

- Prinzipielle Gefahren für VoIP
- Angriffe auf den Medienstrom
- Angriffe auf die Signalisierung
- Angriffe auf die Geräte
- Security-Maßnahmen im LAN und WLAN
- Port Security und Authentisierung nach 802.1X
- Security-Maßnahmen im WAN
- Identität bei VoIP (SIP-Identity)
- Lokale Authentisierung und über Proxy-Ketten
- Probleme mit Zertifikaten
- SIPS und S/MIME
- SRTP und SRTCP
- Schlüsselmanagement mit SDES, ZRTP, DTLS und MIKEY
- WebRTC
- VoIP und IPSec
- NAT-Lösungen: STUN, TURN und ICE
- Firewalls und VoIP
- Session Border Controller
- SIP-Connect 2.0

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket aus der Reihe ExperTeach Networking – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

**Zielgruppe**

Der Kurs wendet sich an Planer und Techniker, die für die Konzeption und Realisierung von VoIP-Installationen zuständig sind.

**Voraussetzungen**

Gute Kenntnisse der TCP/IP-Protokollfamilie und gängiger LAN-Technologien sind erforderlich. Die Teilnehmer müssen mit Security-Konzepten wie Verschlüsselung und Authentisierung vertraut sein. Diese können z.B. im Kurs Security in IP-Netzen – Sicherheitslücken erkennen und schließen erlernt werden. Zusätzlich wird ein solides Grundwissen zu VoIP vorausgesetzt.

**Dieser Kurs im Web**

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/**SEVO**

**Vormerkung**

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

**Garantierte Kurstermine**

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

**Ihr Kurs maßgeschneidert**

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

| Training | | Preise zzgl. MwSt. |
|---|---|---|
| **Termine in Deutschland** | **3 Tage** | **€ 1.995,-** |
| **Termine in Österreich** | **3 Tage** | **€ 1.995,-** |
| **Online Training** | **3 Tage** | **€ 1.995,-** |

**Termin/Kursort** — Kurssprache Deutsch

| | | | |
|---|---|---|---|
| 22.05.-24.05.24 | HY Hamburg | 30.09.-02.10.24 | HY Online |
| 22.05.-24.05.24 | HY Online | 30.09.-02.10.24 | HY Wien |
| 22.07.-24.07.24 | HY München | 18.11.-20.11.24 | HY Frankfurt |
| 22.07.-24.07.24 | HY Online | 18.11.-20.11.24 | HY Online |

Stand 29.02.2024

# Inhaltsverzeichnis

## Security für VoIP – Verschlüsselung, Authentisierung und Firewalls


**1 Grundlagen**
1.1 Einleitung
1.2 VoIP-Infrastruktur
1.2.1 Endgeräte
1.2.2 VoIP im Enterprise-Umfeld
1.2.3 IP Centrex
1.2.4 VoIP für Privatkunden
1.2.5 SIP Trunking
1.3 VoIP über das Internet
1.4 WebRTC
1.5 Session Initiation Protocol (SIP)
1.5.1 Adressierung
1.5.2 Aufgaben von SIP Proxys
1.5.3 Die Requests von INVITE bis BYE
1.5.4 Ein Session-Aufbau im Detail
1.5.5 Sicherheitsrelevante Felder
1.5.6 Der Message Body
1.5.7 Session Description Protocol

**2 Angriffe auf VoIP**
2.1 Prinzipielle Gefahren für VoIP
2.2 Angriff auf die Vertraulichkeit
2.2.1 Sniffing und Man in the Middle Attacks
2.2.2 Ermittlung von Kenngrößen
2.3 Angriffe auf die Integrität
2.3.1 Angriff auf den Medienstrom
2.3.2 Angriff auf die Signalisierung
2.4 Angriffe auf die Geräte
2.4.1 Denial of Service
2.4.2 Buffer Overflow
2.4.3 Trojanische Pferde etc.
2.4.4 Theft of Service
2.4.5 Spam for IP Telephony (SPIT)
2.5 Fazit
2.6 Ziele von Security bei VoIP
2.6.1 Vertraulichkeit
2.6.2 Datenintegrität
2.6.3 Authentizität
2.6.4 Verfügbarkeit

**3 Absichern der Verbindungen**
3.1 Security-Grundlagen
3.1.1 Verschlüsselung
3.1.2 Zertifikate
3.1.3 Integrität über Hash-Werte
3.2 Besonderheiten bei VoIP
3.3 Authentisierung
3.3.1 Initiale Authentisierung
3.3.2 Integrität der Folgepakete
3.3.3 Authentisieren mit Pre-Shared Key
3.3.4 Identität bei VoIP
3.3.5 Register mit Authentisierung
3.3.6 SIP Identity
3.4 Absichern des Medienstroms
3.4.1 SRTP und SRTCP – Paketformate
3.4.2 Verschlüsselung bei SRTP
3.4.3 Authentisierung bei SRTP
3.4.4 Key Management von SRTP
3.4.5 Key Management
3.4.6 Schlüsselmanagement für die Signalisierung
3.4.7 Schlüsselmanagement im Session Description Protocol
3.4.8 MIKEY
3.4.9 ZRTP
3.4.10 KMS-basierte Schlüsselverteilung
3.4.11 DTLS-basierter Schlüsselaustausch
3.4.12 T.38 und Security
3.4.13 MSRP und Security
3.5 Absichern der Signalisierung
3.5.1 SIP und TLS
3.5.2 S/MIME
3.5.3 SIP und IPsec
3.6 VPN-Lösungen

**4 Sicherheitsmaßnahmen im Enterprise-Umfeld**
4.1 VoIP im LAN
4.1.1 VLANs
4.1.2 Das Telefon als Switch
4.2 Security-Maßnahmen im LAN
4.2.1 Voice VLANs
4.2.2 Port Security
4.2.3 Authentisierung mit IEEE 802.1X
4.3 Mobile Mitarbeiter
4.4 Inbetriebnahme von Hardphones

**5 VoIP-Security im Providernetz**
5.1 Architektur der IMS Security im Überblick
5.1.1 Wer mit wem im IMS?
5.1.2 Identitäten im IMS
5.1.3 Authentication and Key Agreement: Erste Wahl im IMS
5.1.4 IMS AKA: Der Ablauf
5.1.5 SIP Digest
5.1.6 NASS-IMS-Bundled Authentication (NBA)
5.2 Generic Bootstrapping Architecture
5.3 RCS
5.3.1 Auto-Konfiguration
5.3.2 Registrierung
5.4 SIP-Trunking
5.4.1 Registration Mode
5.4.2 Static Mode
5.4.3 Identität

**6 Integration in die Security-Infrastruktur**
6.1 Session Border Controller
6.1.1 Architektur
6.1.2 SBC im IP Multimedia Subsystem (IMS)
6.1.3 Enterprise-SBC
6.2 VoIP und Firewalls
6.2.1 State Tables
6.2.2 Application Layer Gateway
6.3 VoIP und NAT
6.3.1 NAT und VoIP
6.3.2 Hosted NAT (Latching)
6.3.3 STUN
6.3.4 TURN
6.3.5 Interactive Connectivity Establishment (ICE)
6.4 NAT und Early Media



**ExperTeach Gesellschaft für Netzwerkkompetenz mbH**
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de