Angriffe gegen VoIP/UC-Infrastrukturen

Praxiskurs zu Angriffsverfahren und Schutzmaßnahmen

Kursbeschreibung

Neben der traditionellen Telefonie sind auch Audio/Videokonferenzen, Chats, Softphones, Kommunikation über Browser Elemente der Kommunikation. Die aus diesem Verbund resultierenden, teilweise hochkomplexen VoIP- und UC-Szenarien sind risikoreich und können auch die angrenzenden Unternehmensinfrastruktur akut gefährden.

Im Rahmen der zweitägigen, als Workshop ausgelegten Schulung wird die Perspektive eines Angreifers eingenommen. Die Teilnehmer werden Gespräche belauschen, Verschlüsselungsverfahren aufbrechen, Schutzmaßnahmen umgehen, Zugriff auf Geräte und Systeme erlangen sowie ihre Rechte ausweiten.

Der Workshop soll einen tieferen Einblick in die Vorgehensweise von Angreifern geben, damit die Kursteilnehmer bei der Nachbereitung die Risiken in Netzwerken identifizieren, einschätzen und minimieren können. Theoretische Konzepte werden erläutert und erlernte Angriffsvektoren anhand von praxisbezogenen Übungen erprobt.

Trainer

Moritz Abrell, Senior IT-Security Consultant, SySS GmbH

Dauer

2 Tage

Format

Präsenz-Schulung mit Übungen

Max. Teilnehmer

12 Personen

Kontakt

Frau Julia Noglik
noglik@vaf.de / 02103 700-253

Zielgruppe

- ITK-Techniker
- VoIP-Administratoren

Lernziele

- Aktuelle Bedrohungen und Angriffsvektoren auf VoIP (er)kennen und verstehen
- Risiken in VoIP-Netzen erkennen, einschätzen und minimieren

Know-how-Voraussetzungen

- Grundkenntnisse zu lokalen Netzen (LAN), TCP/IP, SIP

Technisches Equipment

- Übungsrechner und Schulungsnetz werden vom Veranstalter gestellt.

Agenda / Inhalte

Technische Grundlagen

- Unified Communication und Voice-over-IP
- Einführung in die Technologien (SIP, RTP, WebRTC u. a.)
- Terminologie und Aufbau
- Verschlüsselungsverfahren

Angriffsverfahren

- Man-in-the-Middle-Angriffe
- Angriffe gegen Authentisierungsverfahren
- Angriffe gegen Verschlüsselungsverfahren
- Autodeployment- und Provisionierungsangriffe
- Angriffe gegen die Vertraulichkeit von Daten
- SIP Trunking-Angriffe
- Interactive Connectivity Establishment (ICE)-Angriffe
- Angriffe gegen Session Border Controller (SBC)

Schutzmaßnahmen

- Erkennungsmöglichkeiten
- IT Security-Prinzipien
- Konfigurationsempfehlung
- Best Practices

Zum Trainer

Moritz Abrell, Senior IT-Security Consultant, SySS GmbH

Moritz Abrell hat eine telekommunikationstechnische Ausbildung und ist Senior IT-Security Consultant für das IT-Sicherheitsunternehmen SySS GmbH in Tübingen. Er beschäftigt sich täglich mit IT-Sicherheitsanalysen sowie der Identifizierung und Ausnutzung von Schwachstellen in Hard- und Software. Dabei liegt sein Tätigkeitsschwerpunkt im Bereich von VoIP/UC-Systemen. Er ist zudem regelmäßig auf internationalen IT-Sicherheitskonferenzen wie z. B. der DEFCON in Las Vegas vertreten, in denen er von seinen Sicherheitsforschungen berichtet.