IPv6 und Security

Netze und Endgeräte richtig absichern

Die Einführung von IPv6 wirft für Provider, für Enterprise-Netzbetreiber und Privatkunden neue Security-Fragen auf. Gibt es doch mit IPv6 neue Möglichkeiten, ein Netzwerk zu kompromittieren. Zum einen sind es Abarten bereits bestehender Angriffsarten, zum anderen reißt IPv6 neue Sicherheitslücken auf. Um ein IPv6 Netzwerk zu schützen, muss neben diesen grundlegenden Sicherheitsfragen geklärt werden, ob die bislang verwendeten Komponenten wie Firewalls, Proxys oder IPS für IPv6 ausgerüstet sind. Wie wird eine Migration aus Sicht der Security richtig durchgeführt? Was ändert sich nach dem Wegfall von NAT durch die permanente Erreichbarkeit durch öffentliche Adressen? Dieser IPv6 Security Kurs gibt einen detaillierten Überblick über diese brandaktuellen Fragen. Die Teilnehmer lernen, die Gefährdungslage durch IPv6 für ihr Netzwerk einzuschätzen und eine umfassende Absicherung zu planen.

Kursinhalt

- Neue Angriffspunkte durch IPv6
- IPv6-Adressierung absichern
- Die Hilfsprotokolle ICMPv6 und DHCPv6 aus Sicherheitssicht
- IPv6 und First Hop Security
- IPv6-Netzwerke sichern
- Absicherung von Endgeräten
- Router bei IPv6 absichern
- Firewalls an IPv6 anpassen
- Die Migration absichern

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

Der Kurs eignet sich für Planer, Administratoren und Security-Beauftragte, die eine Migration hin zu IPv6 planen, vorbereiten oder begleiten möchten.

Voraussetzungen

Die Teilnehmer benötigen solide Kenntnisse der herkömmlichen IP-Welt und müssen mit IPv6 gut vertraut sein. Ein vorheriger Besuch des Kurses IPv6 – Adressierung, Routing und IPv4-Interworking ist unbedingt anzuraten. Weiterhin wird vorausgesetzt, dass die Teilnehmer gängige Security-Konzepte kennen und verstehen.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/**IP6S**

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	**2 Tage**	**€ 1.595,-**
Termine in Österreich	**2 Tage**	**€ 1.595,-**
Termine in der Schweiz	**2 Tage**	**€ 2.150,-**
Online Training	**2 Tage**	**€ 1.595,-**

Termin/Kursort — Kurssprache Deutsch

05.06.-06.06.25	HY Frankfurt	25.09.-26.09.25	HY Wien
05.06.-06.06.25	HY Online	23.10.-24.10.25	HY Frankfurt
03.07.-04.07.25	HY Hamburg	23.10.-24.10.25	HY Online
03.07.-04.07.25	HY Online	23.10.-24.10.25	Zürich
07.08.-08.08.25	HY München	20.11.-21.11.25	Berlin
07.08.-08.08.25	HY Online	20.11.-21.11.25	HY Hamburg
28.08.-29.08.25	HY Düsseldorf	20.11.-21.11.25	HY Online
28.08.-29.08.25	HY Online	18.12.-19.12.25	HY München
25.09.-26.09.25	HY Online	18.12.-19.12.25	HY Online

Stand 15.04.2025

IPv6 und Security

Inhaltsverzeichnis

IPv6 und Security – Netze und Endgeräte richtig absichern

1 Grundlegende Sicherheitsüberlegungen
1.1 Grundsätzliche Überlegungen
1.1.1 Sicherheitsmaßnahmen
1.1.2 Personal und Dienstleister
1.2 IPv4 und IPv6 – Sicherheit im Vergleich
1.2.1 Die aktuelle Sicherheitslage
1.2.2 Vulnerable IPv6 Stacks
1.3 Der IPv6-Header aus Sicherheitssicht
1.3.1 Das Flow Label – Covert Channel
1.3.2 Extension Header Parsing
1.3.3 Sicherheitsrelevanz der Erweiterungsheader
1.3.4 Die Filterung von IPv6
1.4 Die Sicherheit testen – Tools für IPv6 Vulnerability Tests
1.4.1 IPv6 Port Scanner
1.4.2 Schwachstellenscanner für IPv6
1.4.3 Paket-Generatoren
1.4.4 Die THC Toolsammlung

2 IPv6-Adressierung aus Sicherheitssicht
2.1 Sicherheitsrelevanz von NAT
2.1.1 NAT-Varianten bei IPv4
2.1.2 Ende zu Ende Adressierung bei IPv6
2.1.3 Kein IP-Hiding
2.1.4 IPv6-IPv6 Network Prefix Translation (NPTv6)
2.2 Sicherheitsbetrachtungen zu den Adressarten
2.2.1 EUI 64 – großer Wiedererkennungswert
2.2.2 Temporäre Adressen
2.3 IPv6-Adressen und Netze auskundschaften
2.3.1 Passive Sniffing
2.3.2 Multicast Enumeration
2.3.3 Registrierungs-Abfrage
2.3.4 IPv6 Netze scannen
2.3.5 IPv6-Adressen erraten
2.3.6 DNS Reconnaissance

3 IPv6-LANs Angriffe und Gegenmaßnahmen
3.1 Neighbor-Discovery-Angriffe
3.1.1 Trust Models and Threats
3.1.2 NDP Spoofing
3.1.3 Neighbor Unreachability Detection (NUD)
3.1.4 DoS_New_IP6
3.1.5 NDP Exhaustion Attack
3.1.6 Neighbor Advertisement Flooding
3.2 SLAAC Angriffe
3.2.1 Rogue Router
3.2.2 Man in the Middle mit RAs
3.2.3 Faked Default Gateway
3.2.4 RA Flooding
3.3 DHCPv6 Angriffe
3.3.1 DHCPv6 Starvation
3.3.2 Rogue DHCPv6 Server
3.4 ICMPv6-Angriffe
3.4.1 Amplification Attack
3.4.2 Redirect-Angriffe
3.5 ACLs zur Sicherung
3.5.1 Rogue Router ausgrenzen
3.5.2 Rogue DHCP Server verhindern
3.5.3 RA Guard
3.5.4 DHCPv6 Guard/Shield
3.5.5 NDP Snooping
3.5.6 NDP Inspection
3.6 SEND
3.6.1 SEND und CGA
3.6.2 RAs mit SEND absichern
3.6.3 SEND und Stateful Autoconfiguration
3.7 IPv6 und First Hop Security
3.7.1 MLD-Sicherheit
3.7.2 IEEE 802.1X - LAN Security
3.7.3 MACsec - Ebene 2-Verschlüsselung

4 Router in IPv6 Netzwerken sichern
4.1 IPv6 Filterung
4.1.1 IPv6 ACLs aufsetzen
4.1.2 Eingehender Verkehr
4.1.3 Adressen filtern
4.1.4 ICMPv6 filtern
4.2 Sicherung der Routingprotokolle
4.2.1 Authentisierung bei Routing Protokollen
4.2.2 BGP-4 – Verwendung von Link Local Unicasts
4.2.3 IP Spoofing verhindern
4.3 IPsec in IPv6-Netzen
4.3.1 Einsatzmöglichkeiten von IPsec
4.3.2 Host to Host Szenario
4.3.3 IPv6 VPNs
4.3.4 IPv6-VPDN mit IPsec
4.3.5 IPsec RAS VPNs und IPv6

5 Sicherheitslösungen anpassen - Firewalls & Co.
5.1 IPv6 Fähigkeit hinterfragen
5.2 Filterregeln in Dual Stack Netzen
5.2.1 Ergänzung der Security Policy
5.2.2 Objekte mit multiplen IPv6-Adressen
5.2.3 Zuweisung statischer Adressen per DHCP
5.3 Next Generation Firewalls und Proxies
5.3.1 Probleme mit Content Filtering
5.3.2 Application Filtering
5.3.3 Identity Based Firewall - IP-Unabhängig
5.4 IPv6-IPS
5.4.1 IP-Unabhängigkeit
5.4.2 Neue netzbasierte Regeln
5.5 Hersteller im Vergleich
5.5.1 Check Point
5.5.2 Cisco
5.5.3 Palo Alto
5.5.4 Fortinet
5.5.5 Juniper
5.5.6 Barracuda
5.6 Radius und IPv6
5.6.1 IPv6-Konnektivität herstellen
5.6.2 RADIUS-IPv6-Attribute
5.6.3 Cisco ISE
5.6.4 Microsoft – Network Policy Server
5.6.5 Freeradius und IPv6
5.7 Proxies in IPv6-Netzen
5.7.1 Proxy Varianten
5.7.2 Adress-Umsetzung

6 Sicherheit während der Migration
6.1 Gedanklicher Umzug zu IPv6
6.2 IPv6 Latent Threats
6.3 Dual Stack – Doppelter Schutz notwendig
6.3.1 Endgerätesicherheit aus Sicht von IPv6
6.3.2 Windows
6.3.3 Linux
6.3.4 Mac OS
6.3.5 Mobile Devices
6.4 Tunneltechnologien sichern
6.4.1 Die Tunnel-Sicherheit hinterfragen
6.4.2 Configured Tunnel sichern
6.4.3 Tunnel Traffic verschlüsseln
6.5 Die Migration aus Sicherheitssicht
6.5.1 Adressdesign für ein sicheres IPv6-Netz
6.5.2 Best Practices

A Online-Lab-Übungen
A.1 Lab Übungen im Kurs
A.1.1 Laboraufbau
A.2 Übungen Kapitel 2
A.3 Übungen Kapitel 3

ExperTeach Training & Consulting GmbH
Handelskai 94-96 · 1200 Wien · Telefon: +43 1 2350 383-0 · Fax: +43 1 2350 383-19 · info@experteach.at · www.experteach.at