

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? Welche Lücken werden durch Tunnelmechanismen wie Teredo in neueren Betriebssystemen (Windows 7) aufgerissen ohne dass überhaupt eine Umstellung auf IPv6 erfolgt, und wie sind diese zu schließen? Dieser 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 und die Hilfsprotokolle ICMPv6 und DNSv6
- Migrationsszenarien mit Tunneln und ihre Risiken
- IPv6 und Firewalls
- IPv6 Router absichern
- Providerthemen: Absichern des Routings sowie der Kundenzugänge
- Absicherung von Endgeräten
- VPNs und IPv6
- Mobile IPv6 und Security

Jeder Teilnehmer erhält ausführliche Kursunterlagen aus der Reihe ExperTeach Networking in deutscher Sprache.

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 dem neuen Protokoll gut vertraut sein. Ein vorheriger Besuch des Kurses IPv6 - Adressierung, Routing und IPv4-Interworking ist gegebenenfalls anzuraten. Weiterhin wird vorausgesetzt, dass die Teilnehmer gängige Security-Konzepte kennen und verstehen.



Vormerkung und Buchung

Gerne merken wir für Sie für die Dauer von zwei Wochen kostenfrei und unverbindlich einen Kursplatz vor. Auf www.experteach.de können Sie unter *Anmeldung* bequem Vormerkung, Buchung und Hotelreservierung vornehmen. Oder rufen Sie uns einfach an unter 06074-4868-0.

Für geschlossene Teilnehmergruppen modifizieren wir diesen Kursinhalt gerne entsprechend Ihren Anforderungen. Bitte sprechen Sie uns an!



Auf Wunsch senden wir Ihnen gerne unseren kompletten Katalog zu, der Sie über alle Trainings und andere Dienstleistungen informiert.

2 Tage € 1.195,00 • CHF 1.795,00 • zzgl. MwSt.

Termin/Kursort

24.05.-25.05.12	Frankfurt	25.10.-26.10.12	München
21.06.-22.06.12	Düsseldorf	25.10.-26.10.12	Stuttgart
26.07.-27.07.12	München	22.11.-23.11.12	Zürich
26.07.-27.07.12	Wien	22.11.-23.11.12	Frankfurt
30.08.-31.08.12	Frankfurt	20.12.-21.12.12	Düsseldorf
27.09.-28.09.12	Berlin	24.01.-25.01.13	München
27.09.-28.09.12	Hamburg	21.02.-22.02.13	Frankfurt

Aktuelle Informationen finden Sie auf www.experteach.de IP65



EXPERTeach





1 Grundlegende Sicherheitsüberlegungen

- 1.1 IPv4 und IPv6 – Sicherheit im Vergleich
- 1.2 Derzeitiges Angriffspotential
 - 1.2.1 Informationsbeschaffung
 - 1.2.2 IPv6 Netze auskundschaften
 - 1.2.3 Layer 3 und Layer 4 Spoofing
 - 1.2.4 Mangelnde Applikationssicherheit
- 1.3 Die Sicherheit testen - Tools für IPv6
Vulnerability Tests

2 IPv6 Sicherheit von Protokollen und Abläufen

- 2.1 IPv6 – Das Protokoll und seine Schwächen
 - 2.1.1 Schwächen des Headers
 - 2.1.2 Angriffe durch Erweiterungsheader
 - 2.1.3 Multicast Angriffe
 - 2.1.4 Sicherheitsrelevanz von NAT
- 2.2 Das Hilfsprotokoll ICMPv6
 - 2.2.1 ICMPv6 aus Sicherheitssicht
 - 2.2.2 Neighbor Solicitation
 - 2.2.3 SEND
 - 2.2.4 Router Advertisements
 - 2.2.5 Weitere ICMP-Angriffe
 - 2.2.6 Die Filterung von ICMPv6
- 2.3 DHCPv6
 - 2.3.1 DHCPv6 Details
 - 2.3.2 DHCPv6-Abläufe
 - 2.3.3 Sicherheit von DHCPv6

3 Sicherheit von Geräten und Netzen

- 3.1 IPv6 in Endgeräten
 - 3.1.1 Microsoft
 - 3.1.2 Linux
 - 3.1.3 Sun Solaris
 - 3.1.4 Mac OS X
- 3.2 Router in IPv6 Netzwerken sichern
 - 3.2.1 Access Listen aufsetzen
 - 3.2.2 IPv6-Filter auf Perimeter Routern
- 3.3 Sicherung der Routingprotokolle
 - 3.3.1 RIPng
 - 3.3.2 OSPF
 - 3.3.3 IS-IS
 - 3.3.4 BGP-4

4 Sicherheit während der Migration

- 4.1 Problemfall unvorbereiteter Umstieg
 - 4.1.1 IPv6 Latent Threats
 - 4.1.2 Schutz gegen IPv6
- 4.2 Dual Stack – Zwei Welten
 - 4.2.1 DNS macht's möglich
 - 4.2.2 Schutz gegen Dual Stack-Angriffe
- 4.3 IPv4 zum Transport: Tunnelmechanismen

4.3.1 Wie sicher ist der Tunnel?

- 4.3.2 Statische Tunnel – 6in4
- 4.3.3 Dynamische Tunnel – 6to4
- 4.3.4 6RD
- 4.3.5 In einer Site – ISATAP
- 4.3.6 Teredo
- 4.3.7 Tunnel Broker
- 4.4 NAT64
 - 4.4.1 DNS64
 - 4.4.2 NAT64 – Sicherheitsprobleme

5 IPv6-Sicherheit mit IPsec

- 5.1 IPsec – Sicherheit für IP
 - 5.1.1 IPsec und IPv6
 - 5.1.2 IPsec – Die IPv6-Erweiterungsheader
- 5.2 Internet Key Exchange
 - 5.2.1 Die Phasen von IKEv1
 - 5.2.2 IKEv2 – Schneller und einfacher
- 5.3 IPsec in IPv6-Netzen
 - 5.3.1 Host to Host
 - 5.3.2 Gateway-to-Gateway
 - 5.3.3 IPsec und dynamische Einwahl



ExperTeach Gesellschaft für Netzwerkkompetenz mbH

Waldstr. 94 • D-63128 Dietzenbach
 Telefon +49 6074 4868-0 • Telefax +49 6074 4868-109
 info@experteach.de • www.experteach.de

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 11.05.2012