

Cyber Defense

Firewalls, Proxys und Advanced Protection

Zentrale Bausteine zur Umsetzung einer Sicherheitsrichtlinie sind Firewall, Proxy und IPS. Firewalls sollen typischerweise das interne Netz vor unerwünschten Zugriffen aus dem Internet schützen. Proxys untersuchen die übertragenen Daten im Detail und blockieren oder verändern unerwünschte Inhalte. Intrusion Prevention Systeme (IPS) sollen den Verkehr im Netzwerk analysieren, Angriffe entdecken und Gegenmaßnahmen ergreifen. Die Funktionalität moderner Firewall-Systeme geht weit über einfache Filtertechniken hinaus und kombiniert die verschiedenen Mechanismen.

Dieser Kurs beschäftigt sich mit den grundlegenden Technologien und Arbeitsweisen, auf denen Firewalls, Proxys, IPS basieren. Die Kombination dieser Systeme und Interaktion mit anderen Komponenten bildet einen weiteren Schwerpunkt.

Kursinhalt

- Angriffsszenarien, Vorgehensweisen, Techniken
- Statische Paketfilter, Access-Listen
- Dynamische Paketfilter, Stateful Firewalls
- Layer-2-Firewalling
- Sicherheit in industriellen Netzen
- Personal Firewalls, Endpoint Security, SASE
- Proxys generisch oder als Spezialisten
- Web Proxy
- TLS Proxy
- Mail Relay
- DNS Proxy
- URL Filtering und Application Control
- Authentisierung an Firewall oder Proxy, Active Directory Integration
- DMZ-Konzepte, NAT, VPN, Zusammenspiel mit VoIP
- Hochverfügbarkeit und Lastverteilung
- IPS, IDS – Prevention vs. Detection
- IPS Typen (HIPS, NIPS, CIIPS, WIPS)
- IPS Methoden und weitere HIDS-Techniken
- SIEM-Systeme, XDR

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

Wer in Netzwerkdesign oder Projektmanagement arbeitet, lernt die Wirkungsweise und Umsetzung von Security-Lösungen kennen. Technisches Personal erwirbt das grundlegend technologische Know-how für den Betrieb von Firewalls, Proxys und IPS, auch als Basis für nachfolgende Produktschulungen der einschlägigen Hersteller.

Voraussetzungen

Basiswissen in den Netzwerk- und Internet-Terminologien und insbesondere Kenntnisse der IP-Protokolle sind erforderlich.

Dieser Kurs im Web



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

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,-
Online Training	3 Tage	€ 1.995,-
Termin/Kursort	Kurssprache Deutsch 	
09.10.-11.10.24  Frankfurt	05.02.-07.02.25  Online	
09.10.-11.10.24  Online	26.03.-28.03.25  Düsseldorf	
27.11.-29.11.24  Hamburg	26.03.-28.03.25  Online	
27.11.-29.11.24  Online	21.05.-23.05.25  München	
05.02.-07.02.25  Frankfurt	21.05.-23.05.25  Online	

Stand 30.07.2024



Inhaltsverzeichnis

Cyber Defense – Firewalls, Proxys und Advanced Protection

1 Einführung und Motivation	3.4 Next Generation Firewall	6.3 TLS Proxys
1.1 Angriffe im Netzwerk		6.3.1 Outbound Inspection
1.1.1 Angriffe von Extern	4 Bestandsaufnahme und Planung	6.3.2 Inbound Inspection
1.1.2 Interne Angriffe	4.1 Sicherheitsrichtlinien	6.4 Mail Relays
1.1.3 Social Engineering Attacks	4.1.1 Planerische Aspekte	6.4.1 Missbrauch und Gefahr
1.1.4 Denial of Service Attacks	4.1.2 Die Umsetzung im Detail	6.4.2 E-Mail Security-Konzepte
1.2 Access Control – Filterung im Netzwerk	4.2 Bestandsaufnahme mit System	6.4.3 Schutz gegen Phishing und CEO Fraud
1.2.1 Aufgaben einer Firewall	4.3 Der Preis der Sicherheit – Finanz- und Zeitaufwand	6.5 DNS Proxys
1.2.2 Zusammenspiel mit anderen Netzkomponenten	4.3.1 Hard- und Software-Kosten	6.5.1 Design-Aspekte
1.2.3 Firewall und Proxy im OSI-Modell	4.3.2 Installationsaufwand	6.5.2 Schutz-Maßnahmen
1.3 Das Internet Protokoll	4.3.3 Administrative Kosten	6.6 VoIP – Voice over IP
1.3.1 IPv4 – Header, Format und Funktionen	4.4 Security Policy - Zugriffsregeln erstellen	6.6.1 VoIP Fragestellungen mit NAT und Firewalls
1.3.2 IPv6 – Wichtige Neuerungen	4.4.1 Grundlegende Prinzipien	6.6.2 Lösung 1: Application Layer Gateway
1.3.3 UDP – verbindungslos und ungesichert	4.4.2 Dokumentation	6.6.3 Lösung 2: STUN
1.3.4 TCP – verbindungsorientiert und gesichert	4.5 Logging-Strategien	6.6.4 Lösung 3: Session Border Controller
1.3.5 QUIC – mit UDP und doch gesichert	4.5.1 Das Logging planen und umsetzen	
	4.5.2 Lokales und zentrales Logging	7 Intrusion Prevention Systems
2 Schutz durch Netzdesign	4.5.3 Externe Logserver und SIEM-Systeme	7.1 Intrusion Detection System
2.1 Die Perimeter Firewall	4.6 Redundanz-Aspekte	7.2 Intrusion Prevention System
2.2 DMZ-Konzepte	4.6.1 Firewall-Cluster	7.3 IPS Typen
2.2.1 DMZ – Traffic Flow	4.6.2 Redundanz mit VRRP	7.3.1 Host-based IPS - HIPS
2.2.2 DMZ – Kommunikationsprozesse	4.6.3 Load Sharing	7.3.2 Network-based IPS - NIPS
2.3 Interne Zonen trennen	4.6.4 Load Sharing mit Content Switches	7.3.3 Cloud-based IPS - CIIPS
2.3.1 Bereiche kontrollieren	4.7 Administrative Aufgaben	7.3.4 Wireless-LAN-based IPS - WIPS
2.3.2 Lateral Movement verhindern	4.7.1 Change Mangement	7.4 Detections und Preventions Methoden
2.4 Network Address Translation (NAT) und Firewalls	4.7.2 Das Regelwerk überwachen	7.4.1 Mustererkennung
2.4.1 Hintergründe zu NAT	4.7.3 Backups erstellen	7.4.2 Protokollanalyse
2.4.2 NAT und IPv6	4.7.4 Updates – Planung und Umsetzung	7.4.3 Anomalieerkennung
2.4.3 Probleme mit NAT		7.4.4 HIDS-Techniken
2.4.4 Applikationsanpassungen	5 Firewalls – Paketfilter und mehr	7.5 Baselineing vor und während dem Betrieb
2.5 Firewalls und VPN	5.1 Regelwerke	7.5.1 Den Traffic vorbereiten
2.5.1 Site to Site VPNs	5.1.1 Kriterium - Trigger	7.5.2 IP Fragmentierung ein Beispiel
2.5.2 RA VPNs	5.1.2 Aktionen	7.6 Evasion Techniques
2.5.3 IPsec als Tunnelprotokoll	5.1.3 First Match Prinzip und Performance-Aspekte	7.7 SIEM Systeme
2.5.4 Sicherheit durch TLS	5.1.4 Mehrere Regelwerke	7.7.1 Event-Definitionen, Korrelationen
2.6 Sicherheit in Industriellen Netzen	5.2 Unterschiedliche Firewall-Konzepte	7.7.2 SIEM nützlich, aber kein Allheilmittel
2.6.1 Die Herausforderungen	5.3 URL Filtering und Application Control	7.7.3 SIEM-Produkte
2.6.2 Security Segmentierung in der OT	5.3.1 URL Filtering	7.8 XDR – Extended Detection und Response
2.6.3 Kommunikationsprozesse kontrollieren	5.3.2 Application Control	
2.6.4 OT/IT Integration	5.4 Identity Based Firewall	A Firewall-Produkte
2.6.5 Wartungszugänge realisieren	5.4.1 Kleine Lösungen: Lokale Benutzerdatenbank	A.1 Check Point
2.7 Secure Access Service Edge (SASE)	5.4.2 AD-Integration	A.2 ASA – Cisco Systems
2.7.1 SD-WAN	5.4.3 LDAP	A.3 Firepower – Cisco Systems
2.7.2 SASE POP und SASE Backbone	5.4.4 RADIUS ein AAA-Dienst	A.4 Palo Alto
2.7.3 Security Services im SSE	5.5 Transparente Firewall	A.5 Juniper
	5.6 Personal Firewall	A.6 Fortinet
3 Sicherheitslösungen im Überblick	6 Proxys - Applikationskontrolle im Visier	A.7 Sophos
3.1 Unterschiedliche Security-Devices: Firewall	6.1 Proxy – Stellvertreter für Client und Server	A.8 Genua
3.1.1 Statische Paketfilter	6.1.1 Dedizierte Proxys – Varianten	A.9 Blue Coat Proxy
3.1.2 Stateful Inspection	6.1.2 Generische Proxys – Circuit Level Proxys und SOCKS	A.10 Weitere Anbieter
3.1.3 Application Layer Firewall	6.2 Web Proxys	A.11 AlgoSec u. a. Firewall Analyzer
3.2 Proxy	6.2.1 Explicit vs. Transparent Proxy	A.12 Open Source Firewalls
3.2.1 Trennung der Verbindung	6.2.2 Authentisierung am Proxy	A.13 Open Source Proxy: Squid
3.2.2 Lückenlose Analyse einer Datei vor der Weiterleitung	6.2.3 Schutzmaßnahmen	
3.3 Intrusion Detection und Prevention	6.2.4 Web Application Firewall – Reverse Proxy	
3.3.1 Threat Prevention – Malware Protection		

