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, ClIPS, WIPS)
- IPS Methoden und weitere HIDS-Techniken
- SIEM-Systeme, XDR

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

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.

Stand 07.05.2025

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		Preis	Preise zzgl. MwSt.		
Termine in [Deutschlan	d 3 Tage	€ 1.995,-		
Termine in C	Österreich	3 Tage	€ 1.995,-		
Online Train	ing	3 Tage	€ 1.995,-		
Termin/Kursort		Kurssprache Deutsch			
21.0523.05.25	<u>○N</u> Online	08.1010.10.25	Online		
30.0701.08.25	Frankfurt	26.1128.11.25	Online		
30.0701.08.25	Online	26.1128.11.25	₩Wien		
08.1010.10.25	W Hamburg				



Inhaltsverzeichnis

Cyber Defense – Firewalls, Proxys und Advanced Protection

1	Einführung und Motivation	3.4	Next Generation Firewall		TLS Proxys
1.1	Angriffe im Netzwerk	_			Outbound Inspection
	Angriffe von Extern	4	Bestandsaufnahme und Planung		Inbound Inspection
	Interne Angriffe	4.1	Sicherheitsrichtlinien	6.4	Mail Relays
	Social Engineering Attacks		Planerische Aspekte		Missbrauch und Gefahr
	Denial of Service Attacks		Die Umsetzung im Detail		E-Mail Security-Konzepte
1.2	Access Control – Filterung im Netzwerk	4.2	Bestandsaufnahme mit System		Schutz gegen Phishing und CEO Fraud
	Aufgaben einer Firewall	4.3	Der Preis der Sicherheit – Finanz- und Zeitaufwand	6.5	DNS Proxys
	Zusammenspiel mit anderen Netzkomponenten		Hard- und Software-Kosten		Design-Aspekte
	Firewall und Proxy im OSI-Modell				Schutz-Maßnahmen
1.3	Das Internet Protokoll		Administrative Kosten	6.6	VoIP – Voice over IP
	IPv4 – Header, Format und Funktionen	4.4	Security Policy - Zugriffsregeln erstellen		VoIP Fragestellungen mit NAT und Firewalls
	IPv6 – Wichtige Neuerungen		Grundlegende Prinzipien		Lösung 1: Application Layer Gateway
	UDP – verbindungslos und ungesichert		Dokumentation		Lösung 2: STUN
	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		Das Logging planen und umsetzen	-	Interview Description Contains
			Lokales und zentrales Logging	7	Intrusion Prevention Systems
2	Schutz durch Netzdesign		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		Firewall-Cluster	7.3	IPS Typen
	DMZ – Traffic Flow		Redundanz mit VRRP		Host-based IPS - HIPS
	DMZ – Kommunikationsprozesse		Load Sharing		Network-based IPS - NIPS
2.3	Interne Zonen trennen Bereiche kontrollieren		Load Sharing mit Content Switches		Cloud-based IPS - CIIPS Wireless-LAN-based IPS - WIPS
		4.7	Administrative Aufgaben	7.3.4	Detections und Prevetions Methoden
2.3.2	Lateral Movement verhindern		Change Mangement Das Regelwerk überwachen		Mustererkennung
	Network Address Translation (NAT) und Firewalls Hintergründe zu NAT		Backups erstellen		_
	NAT und IPv6		Updates – Planung und Umsetzung		Protokollanalyse Anomalieerkennung
	Probleme mit NAT	4.7.4	opulates – Flanding und Offisetzung		HIDS-Techniken
	Applikationsanpassungen	5	Firewalls – Paketfilter und mehr	7.4.4	Baselining vor und während dem Betrieb
2.5	Firewalls und VPN	5.1	Regelwerke		Den Traffic vorbereiten
	Site to Site VPNs		Kriterium - Trigger		IP Fragmentierung ein Beispiel
	RA VPNs		Aktionen	7.6	Evasion Techniques
	IPsec als Tunnelprotokoll		First Match Prinzip und Performance-Aspekte	7.7	SIEM Systeme
	Sicherheit durch TLS		Mehrere Regelwerke		Event-Definitionen, Korrelationen
2.6	Sicherheit in Industriellen Netzen	5.2	Unterschiedliche Firewall-Konzepte		SIEM nützlich, aber kein Allheilmittel
	Die Herausforderungen	5.3	URL Filtering und Application Control		SIEM-Produkte
	Security Segmentierung in der OT		URL Filtering	7.8	XDR – Extended Detection und Response
	Kommunikationsprozesse kontrollieren		Application Control		
	OT/IT Integration	5.4	Identity Based Firewall	Α	Firewall-Produkte
	Wartungszugänge realisieren		Kleine Lösungen: Lokale Benutzerdatenbank	A.1	Check Point
2.7	Secure Access Service Edge (SASE)		AD-Integration	A.2	ASA – Cisco Systems
2.7.1	SD-WAN		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			A.7	Sophos
3.1	Unterschiedliche Security-Devices: Firewall	6	Proxys - Applikationskontrolle im Visier	A.8	Genua
3.1.1	Statische Paketfilter	6.1	Proxy – Stellvertreter für Client und Server	A.9	Blue Coat Proxy
3.1.2	Stateful Inspection	6.1.1	Dedizierte Proxys – Varianten	A.10	Weitere Anbieter
	Application Layer Firewall		Generische Proxys – Circuit Level Proxys und SOCKS	A.11	AlgoSec u. a. Firewall Analyzer
3.2	Proxy	6.2	Web Proxys		Open Source Firewalls
3.2.1	Trennung der Verbindung	6.2.1	Explicit vs. Transparent Proxy		Open Source Proxy: Squid



3.2.1 Trennung der Verbindung

3.3 Intrusion Detection und Prevention

3.3.1 Threat Prevention – Malware Protection

3.2.2 Lückenlose Analyse einer Datei vor der Weiterleitung



6.2.1 Explicit vs. Transparent Proxy

6.2.4 Web Application Firewall – Reverse Proxy

6.2.2 Authentisierung am Proxy

6.2.3 Schutzmaßnahmen









A.13 Open Source Proxy: Squid