

Cyber Security

Cyber Threats, Cyber Angriffe und Gegenstrategien

Die digitale Vernetzung in unterschiedlichen Bereichen unserer Gesellschaft schreitet voran. Diesen Umstand machen sich Cyberkriminelle in großem Umfang zunutze, um ihre teilweise hochkomplexen Angriffe auszuführen. Herkömmliche Schutzmaßnahmen geraten in diesem Umfeld an ihre Grenzen.

Modernere Methoden der Cyber Security hingegen bieten einen effektiveren Schutz, lassen der digitalen Welt aber auch Möglichkeit zur Entfaltung. Die Teilnehmer dieses Seminars erhalten Überblick zu diesen Themen und werden in die Lage versetzt, Cyber-Risiken zu bewerten sowie Schutzmaßnahmen und deren Planung einzuordnen.

Kursinhalt

- Spionage, Sabotage, Missbrauch
- Verschiedenen Arten von Angreifern
- Cyber-Risiken
- Verschiedene Angriffstechniken
- Phishing, Mass- vs. Spear Attacks
- Ransomware
- Denial of Service (DoS und DDoS)
- Internet of Things und Industrie 4.0
- Cloud Security
- Advanced Persistent Threats
- Social Engineering
- Security Awareness
- Information Security Management Systems (ISMS)
- BSI-Grundschutz
- KRITIS, NiS und RCE
- CERT
- Next Generation Firewalls
- VPN
- Proxies
- Intrusion Detection und Prevention
- Sandboxing
- Identity Based Access
- First Hop Security
- Endpoint Security
- Bring Your Own Device
- Cyber Security Vulnerability Assessments
- Penetration Tests
- Digitale Forensik
- Security Information and Event Management (SIEM)
- Computer Security Incident Response Team (CSIRT)

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

Zielgruppe

Dieser Kurs wendet sich an die Personen einer Firma, die im Bereich Sicherheit mit dem Schutz vor den Gefahren der modernen digitalen Welt betraut sind oder in diesen Tätigkeitsbereich neu einsteigen.

Voraussetzungen

Idealerweise haben die Teilnehmer bereits Grundkenntnisse in den Bereichen Netzwerktechnologie und Datenkommunikation gesammelt. Der Kurs Moderne IP- & Netzwerkkonzepte – Alles Wesentliche für Sales & Marketing! ist hierfür eine gute Vorbereitung.

Dieser Kurs im Web



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

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,-
Online Training	2 Tage	€ 1.595,-
Termin/Kursort	Kursprache Deutsch	
28.07.-29.07.25 Frankfurt	02.02.-03.02.26 Frankfurt	
28.07.-29.07.25 Online	02.02.-03.02.26 Online	
06.10.-07.10.25 Hamburg	20.04.-21.04.26 München	
06.10.-07.10.25 Online	20.04.-21.04.26 Online	
24.11.-25.11.25 Online	15.06.-16.06.26 Düsseldorf	
24.11.-25.11.25 Wien	15.06.-16.06.26 Online	

Stand 23.05.2025



EXPERTeach



Inhaltsverzeichnis

Cyber Security – Cyber Threats, Cyber Angriffe und Gegenstrategien

1 Die Gefahrenlage einschätzen	3.2.2 Clients absichern	5 Die Sicherheit hinterfragen
1.1 Ziele der Angreifer	3.2.3 Kommunikationswege überwachen	5.1 Sicherheitsmaßnahmen überwachen
1.1.1 Sabotage	3.2.4 Server absichern	5.1.1 Logging-Daten auswerten
1.1.2 Spionage	3.3 Security-Awareness-Maßnahmen	5.1.2 Monitoring der Sicherheitssysteme
1.1.3 Missbrauch	3.3.1 Die Benutzer einbinden	5.2 IT-Prozesse überprüfen – IS Revision
1.2 Arten von Angreifern	3.3.2 Gründe offenbaren	5.2.1 Leitfaden des BSI
1.2.1 Freizeithacker	3.3.3 Einschränkungen begreifbar machen	5.2.2 IS-Revision – Ablauf
1.2.2 Professionelle Angreifer	3.4 Information Security Management Systeme	5.3 Vulnerability Checks
1.2.3 Politische Motive	3.4.1 Hintergründe zu ISMS	5.3.1 Hintergründe der Schwachstellenanalyse
1.2.4 Wirtschaftliche Interessen	3.4.2 Phasen des ISMS	5.3.2 Arten von Schwachstellenanalysen
1.2.5 Cyberterrorismus	3.4.3 ISMS im BSI-Grundschutz	5.3.3 Interne vs. Externe Tests
1.3 Bedrohungen kennen	3.4.4 KRITIS	5.3.4 Compliance Checks
	3.4.5 NIS2 und RCE	5.3.5 Ergebnisse hinterfragen
2 Angriffspunkte erkennen	4 Schutzmaßnahmen umsetzen	5.4 Penetrationstests
2.1 Angriff auf Netzwerke	4.1 Firewalls und Next Generation Firewalls	5.4.1 Einen Angriff simulieren
2.2 Angriff auf Server	4.1.1 Regelwerke erstellen	5.4.2 Ziele von Penetrationstests
2.2.1 Exploitation Attacks	4.1.2 Virtual Private Networks – VPN	5.4.3 Rechtliche Überlegungen
2.2.2 Kennwort-Angriffe	4.1.3 Aufgaben von Next Generation Firewalls	5.4.4 Social Engineering Tests
2.2.3 Applikationsangriffe	4.1.4 Content Awareness	5.4.5 Black Box vs. White Box Tests
2.3 Client Site Attacks	4.1.5 URL-Filtering	
2.3.1 Den Schadcode zustellen	4.1.6 SSL/TLS Inspection	6 Angriffe erkennen
2.3.2 QR-Codes	4.1.7 Identity Based Access	6.1 Verhaltensanalyse
2.3.3 Angriff über schädliche Dokumente	4.1.8 Firewalls in virtualisierten Umgebungen	6.1.1 Kommunikation mit verdächtigen Sites
2.3.4 Ransomware – DoS auf Clients	4.2 Proxy Server	6.1.2 Ungewöhnliche Protokollaktivitäten
2.3.5 Cryptojacking	4.3 IDS und IPS-Systeme	6.1.3 Außergewöhnliche Kommunikationswege
2.4 Mobile Endgeräte angreifen	4.3.1 IDS/IPS-Varianten	6.1.4 Verdächtiges Verhalten
2.5 Social Engineering	4.3.2 Signature Based Protection	6.1.5 Häufung von Alarmmeldungen
2.5.1 Phishing	4.3.3 Protokollanalyse	6.1.6 Verdächtige Login-Versuche
2.5.2 Einen Webserver nutzen	4.3.4 Anomalie Detection	6.2 Security Information and Event Management – SIEM
2.6 Angriffe im Internet of Things	4.3.5 Advanced Evasion Techniques Schutz	6.2.1 Relevante Daten erkennen
2.7 Cloud Security	4.4 Advanced Threat Protection	6.2.2 Meldungen korrelieren
2.7.1 Datenschutz und Compliance	4.4.1 Threat Emulation – Sandboxing	6.3 Digitale Forensik
2.7.2 Account Hijacking	4.4.2 Threat Extraction	6.3.1 Computer Forensik
2.8 Advanced Persistent Threats	4.5 First Hop Security	6.3.2 Netzwerk Forensik
2.8.1 Konzept eines APTs	4.5.1 Sicherheit in LAN und WLAN	6.3.3 Cloud Forensik
2.8.2 Mehrstufiger Angriff	4.5.2 Herkömmliche Sicherheitsfeatures	6.4 Computer Security Incident Response Team – CSIRT
2.8.3 Von Innen angreifen	4.5.3 IEEE 802.1X – Port-basierte Authentisierung	6.4.1 Aufgaben des CSIRT
2.8.4 APT – Schutzmaßnahmen	4.6 Endpoint Security	6.4.2 Sicherheitsrelevante Bereiche definieren
2.8.5 Watering Hole Attacks	4.6.1 Personal Firewalls	6.4.3 Skills der Mitarbeiter
3 Schutzmaßnahmen planen	4.6.2 Malware Protection	6.5 Reaktion
3.1 Kommunikationswege offenlegen	4.6.3 Data Loss Prevention	6.5.1 Probleme beseitigen
3.1.1 Kommunikationspartner erkennen	4.6.4 Disk Encryption	6.5.2 Sicherheitseinstellungen anpassen
3.1.2 Motive hinterfragen	4.6.5 Patch Management	6.5.3 Mitarbeiter schulen
3.2 Sicherheitsrichtlinien erstellen	4.7 BYOD sicher umsetzen	
3.2.1 Benutzerrechte hinterfragen		

