

# Cyber Security

## Cyber Threats, Cyber Angriffe und Gegenstrategien

In der modernen Gesellschaft gewinnt die digitale Vernetzung in unterschiedlichen Lebensbereichen zunehmend an Bedeutung. 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 effektiven Schutz, lassen der digitalen Welt aber auch Möglichkeit zur Entfaltung. Die Teilnehmer dieses Seminars werden in die Lage versetzt, Cyber-Risiken zu bewerten sowie Schutzmaßnahmen und ihre Umsetzung zu planen.

### Kursinhalt

- Internet of Things
- Unified Communication
- Industrie 4.0
- Cloud Security
- Cyber-Risiken
- Spionage, Sabotage, Missbrauch
- Mass- vs. Spear Attacks
- Advanced Persistent Threats
- Security Awareness
- Information Security Management Systems (ISMS)
- Security Information and Event Management (SIEM)
- Computer Security Incident Response Team
- Cyber Security Vulnerability Assessments
- Penetration Tests
- Next Generation Firewalls
- Intrusion Detection und Prevention
- Identity Based Access
- Bring Your Own Device
- Profiling
- Posture Assessment

**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

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.

### Voraussetzungen

Idealerweise haben die Teilnehmer bereits Grundkenntnisse in den Bereichen Netzwerktechnologie und Datenkommunikation, speziell im Bereich LAN und TCP/IP 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.at/go/CYSE](http://www.experteach.at/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.	
<b>Termine in Deutschland</b>		<b>2 Tage</b>	<b>€ 1.595,-</b>
<b>Termine in Österreich</b>		<b>2 Tage</b>	<b>€ 1.595,-</b>
<b>Online Training</b>		<b>2 Tage</b>	<b>€ 1.595,-</b>
<b>Termin/Kursort</b>	<b>Kurssprache Deutsch </b>		
07.10.-08.10.24  Online	03.02.-04.02.25  Online		
07.10.-08.10.24  Wien	24.03.-25.03.25  Düsseldorf		
02.12.-03.12.24  Hamburg	24.03.-25.03.25  Online		
02.12.-03.12.24  Online	19.05.-20.05.25  München		
03.02.-04.02.25  Frankfurt	19.05.-20.05.25  Online		

Stand 14.07.2024



# Inhaltsverzeichnis

## Cyber Security – Cyber Threats, Cyber Angriffe und Gegenstrategien

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

