

Cyber Security

Detecting Attacks and Taking Counter-Measures

In modern society, digital networking is increasingly gaining significance on the most diverse sectors of life. Cyber criminals make liberal use of this fact in order to carry out their in part highly complex attacks. In this environment, conventional protection measures quickly reach their limits. Modern cyber security methods, however, offer efficient protection, while also providing the digital world with options of development. This seminar enables its students to evaluate cyber risks and plan protection measures along with their implementation.

Course Contents

- Internet of Things
- Unified Communication
- Industry 4.0
- Cloud Security
- Cyber Risks
- Espionage, Sabotage, Misuse
- 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 and Prevention
- Identity-Based Access
- Bring Your Own Device
- Profiling
- Posture Assessment

E-Book You will receive the comprehensive documentation package of the ExperTeach Networking series – printed documentation, e-book, and personalized PDF! As online participant, you will receive the e-book and the personalized PDF.

Target Group

This course addresses the employees of a company who are responsible for protection against the hazards of the modern digital world in the field of security.

Prerequisites

Ideally, participants already have a basic know-how in the fields of networking technology and data communications, particularly on the sectors LAN and TCP/IP.

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

www.experteach-training.com/go/CYSE

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
Classes in Germany	2 Days	€ 1,595
Classes in Austria	2 Days	€ 1,595
Online Training	2 Days	€ 1,595
Date/course venue	Course language German	
02/05-03/05/24	Frankfurt	07/10-08/10/24
02/05-03/05/24	Online	07/10-08/10/24
08/07-09/07/24	Frankfurt	02/12-03/12/24
08/07-09/07/24	Online	02/12-03/12/24

Status 04/13/2024



EXPERTeach



Table of Contents

Cyber Security – Detecting Attacks and Taking Counter-Measures

1 Assessing the threat situation	3.1.1 Identifying communication partners	4.6.1 Personal firewalls
1.1 Targets of the attackers	3.1.2 Question motives	4.6.2 Malware Protection
1.1.1 Sabotage	3.2 Create security guidelines	4.6.3 Data Loss Prevention
1.1.2 Espionage	3.2.1 Questioning user rights	4.6.4 Disk Encryption
1.1.3 Abuse	3.2.2 Secure clients	4.6.5 Patch management
1.2 Types of attackers	3.2.3 Monitor communication paths	4.7 Implementing BYOD securely
1.2.1 Recreational hackers	3.2.4 Secure servers	5 Questioning security
1.2.2 Professional attackers	3.3 Security awareness measures	5.1 Monitoring security measures
1.2.3 Political motives	3.3.1 Involve users	5.1.1 Evaluating logging data
1.2.4 Economic interests	3.3.2 Reveal reasons	5.1.2 Monitor security systems
1.2.5 Cyberterrorism	3.3.3 Making restrictions comprehensible	5.2 Review IT processes - IS revision
1.3 Knowing threats	3.4 Information security management systems	5.2.1 Guideline of the BSI
2 Identifying points of attack	3.4.1 Background to ISMS	5.2.2 IS Revision - Procedure
2.1 Attack on networks	3.4.2 Phases of the ISMS	5.3 Vulnerability checks
2.2 Attack on servers	3.4.3 ISMS in BSI basic protection	5.3.1 Background of vulnerability analysis
2.2.1 Exploitation Attacks	4 Implementing protective measures	5.3.2 Types of vulnerability analysis
2.2.2 Password attacks	4.1 Firewalls and Next Generation Firewalls	5.3.3 Internal vs. external tests
2.2.3 Application attacks	4.1.1 Creating rules and regulations	5.3.4 Compliance checks
2.3 Client site attacks	4.1.2 Virtual Private Networks - VPN	5.3.5 Questioning results
2.3.1 Delivering malicious code	4.1.3 Tasks of next generation firewalls	5.4 Penetration tests
2.3.2 QR codes	4.1.4 Content awareness	5.4.1 Simulating an attack
2.3.3 Attack via malicious documents	4.1.5 URL filtering	5.4.2 Objectives of penetration tests
2.3.4 Ransomware - DoS on clients	4.1.6 SSL inspection	5.4.3 Legal considerations
2.3.5 Cryptojacking	4.1.7 Identity Based Access	5.4.4 Social engineering tests
2.4 Attacking mobile devices	4.1.8 Firewalls in virtualized environments	5.4.5 Black box vs. white box tests
2.5 Social engineering	4.2 Proxy server	6 Detecting attacks
2.5.1 Phishing	4.3 IDS and IPS systems	6.1 Behavioral analysis
2.5.2 Using a web server	4.3.1 Types of IDS/IPS	6.1.1 Internal communication to suspicious sites
2.6 Attacks on the Internet of Things	4.3.2 Signature Based Protection	6.1.2 Unusual log activities
2.7 Cloud security	4.3.3 Protocol Analysis	6.1.3 Unusual communication paths
2.7.1 Data protection and compliance	4.3.4 Anomaly Detection	6.1.4 Suspicious behavior
2.7.2 Account hijacking	4.3.5 Protection against Advanced Evasion Techniques	6.1.5 Accumulation of alert messages
2.8 Advanced Persistent Threats	4.4 Advanced Threat Protection	6.1.6 Suspicious login attempts
2.8.1 Concept of an APT	4.4.1 Threat Emulation - Sandboxing	6.2 Security Information and Event Management - SIEM
2.8.2 Multi-stage attack	4.4.2 Threat Extraction	6.2.1 Detecting relevant data
2.8.3 Attacking from the inside	4.5 First Hop Security	6.2.2 Correlating messages
2.8.4 APT protective measures	4.5.1 Security in LAN and WLAN	6.3 Digital forensics
2.8.5 Watering hole attacks	4.5.2 Traditional security features	6.3.1 Computer forensics
3 Planning protective measures	4.5.3 IEEE 802.1X - Port-based authentication	6.3.2 Network Forensics
3.1 Disclose communication channels	4.6 Endpoint Security	6.3.3 Cloud Forensics

