

Technical and Operational IT Security Concepts

Course Code: DLBCSEEISC01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-Systems and Networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructure require higher security mechanism regarding confidentiality, integrity and availability. Based on specific "Protection Profiles" high sophisticated tools, mechanisms and procedures need to be designed, implemented, configured and operated. With this course the student will be able to evaluate given IT-Infrastructure, support the security-design of new IT-Systems and Networks by developing specific Protection Profiles, evaluate which technical and operational security measures and application are required and how these are integrated, configured and operated.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Contents

1. Network Analysis and Evaluation
 - 1.1 Layer Specific Threats and Vulnerabilities
 - 1.2 DATA Flow, Interdependencies and Interrelationships
 - 1.3 Vulnerability Scanning and Detection
 - 1.4 Supporting Tools and Techniques

2. Protection Profiles
 - 2.1 Reference Architecture Technology and Networking
 - 2.2 Risk Assessment, Residual Risk and Risk Management
 - 2.3 Security Requirements and Safeguards
 - 2.4 Security Evaluation of IT-Security Products
 - 2.5 Accreditation of IT-Systems and Networks
3. Intrusion Detection Systems
 - 3.1 Detection Strategy
 - 3.2 Data Sources, Sensors
 - 3.3 Analytics
 - 3.4 Indicators of Compromise
4. Network Monitoring
 - 4.1 Threat Protection Systems
 - 4.2 Wireless Sensor Networks Technology
 - 4.3 Threat Information Sharing
5. Security Information and Event Management (SIEM)
 - 5.1 Technical and Operational DATA Sources
 - 5.2 DATA Fusion
 - 5.3 Network Norm Behavior
 - 5.4 Big Data Analysis – Transferring Technical Data for Operational Information
 - 5.5 Security Situation Picture, Situational Awareness
 - 5.6 Incident Response Strategies and Automated Responses
6. IT-Security Evaluation and Assessment
 - 6.1 IT-Security Metrics
 - 6.2 IT-Security Assessment

Literature**Compulsory Reading****Further Reading**

- Federal Office for Information Security (BSI) (2018): IT-Grundschutz Profiles - Structural Description - COMMUNITY DRAFT.
- Hayden, L. (2010): IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Education, New York City, NY.
- McNab, C. (2016): Network Security Assessment: Know Your Network. 3. Auflage, O'Reilly UK Ltd., London.
- Miller, D. R. et al. (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, New York City, NY.

Study Format Distance Learning

Study Format Distance Learning	Course Type Online Lecture
--	--------------------------------------

Information about the examination	
Examination Admission Requirements	BOLK: yes Course Evaluation: no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study 90 h	Contact Hours 0 h	Tutorial 30 h	Self Test 30 h	Independent Study 0 h	Hours Total 150 h

Instructional Methods	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides