Technical Security

Allgemeine Angaben

Kürzel	TES
Modulverantwortliche	Prof. Dr. E. Koch, Prof. Dr. R. Schumann
Dozenten	Prof. Dr. E. Koch, Prof. Dr. R. Schumann, Prof. Dr. Stehr
Lehrsprache	Deutsch
Semester	4
ECTS	5
Kontaktstunden	40
Selbststudium	85
Dauer	1 Semester
Art	Pflicht in der Spezialisierung „Cyber Security“
Häufigkeit	Jedes Studienjahr
Gewichtung	5/180
Prüfungsleistung	K**R**S90

Stichwörter

- Hacking
- Intrusion Detection
- Penetration Testing
- Cyber Security Framework (CSF)
- Open Web Application Security (OWASP)
- Social Cyber Security
- Blockchain

Zugangsvoraussetzungen

- Wirtschaftsmathematik
- Grundlagen der Informatik

Verwendbarkeit

- Spezialisierungsmodul Digital Transformation
- Spezialisierungsmodul IT-Compliance, Prozesse und Architekturen
- Konsekutive Master-Studiengänge

Qualifikations- und Kompetenzziele

Die Studierenden erlangen grundlegende Kenntnisse der unterschiedlichen technischen Aufgabenbereiche der Cyber Security. Dazu gehören u. a. das Verstehen der Vorgehensweisen bei der Penetration technischer Systeme sowie die Klassifizierung unterschiedlicher Bedrohungstypen. Anhand von Fallbeispielen und Übungen werden reale Szenarien analysiert und diskutiert. Es werden Sicherheitsarchitekturen vorgestellt und erläutert. Weiterhin werden Grundkonzepte zur Sicherung technischer Systeme bis hin zur Entwicklung technischer Gegenmaßnahmen erörtert sowie Frameworks und Tools im Bereich der Cyber Security kennengelernt.

Lehr- und Lernmethoden

Klassischer Vortrag, Durchführung von Übungen mit Präsentation der Ergebnisse, Fallstudienarbeit, praktische Übungen.

Inhalte

- Grundlagen zu Cyber Security
    - Cyber Risks
    - Cyber Security Landscape
    - Cyber Security Lifecycle
    - Theoretische Grundlagen von Cyber Security
- Techniken und Methoden im Bereich Cyber Security
    - Hacking-Terminologien
    - Ethical Hacking
    - Threat Modelling
    - Vulnerability Analysis
    - Intrusion Detection
    - Penetration Testing
- Techniken und Methoden im Bereich Cyber Security
    - Hacking-Terminologien
    - Ethical Hacking
    - Threat Modelling
    - Vulnerability Analysis
    - Intrusion Detection
    - Penetration Testing
- Tools und Frameworks
    - Klassifikation und Strukturierung von Hacking Tools
    - Hacking Tools (z. B. Kali Linux)
    - Cyber Security Framework (CSF)
    - Open Web Application Security (OWASP)
- Trends und aktuelle Entwicklungen (Auswahl von möglichen Anwendungsfällen)
    - Cloud Security
    - Blockchain und Cyber Security
    - Social Cyber Security
    - Cyber Security im Internet of Things

In Abhängigkeit von aktuellen Entwicklungen können andere Beispiele herangezogen werden.

Grundlegende Literatur:

ANDERSON, Ross: *Security Engineering, 2nd Edition*, Wiley, 2008

MEEUWISSE, Raef: *Cybersecurity for Beginners (2nd Edition),* CyberSimplicity Ltd, London 2017

Ergänzende Literatur:

Scott, James: *Cybersecurity 101: What you absolutely must now*, 2016

ENGEBRETSON, Patrick: *Hacking Handbuch*, Franzis, München 2015

ENISA Threat Landscape Report 2016, EU