

Lehrveranstaltung

IS - IT-Sicherheit

Version: 3 | Letzte Änderung: 05.04.2022 17:30 | Entwurf: 0 | Status: vom verantwortlichen Dozent freigegeben

^ Allgemeine Informationen

Langname	IT-Sicherheit
Anerkennende LModule	<u>IS_MaCSN, IS_MaTIN</u>
Verantwortlich	Prof. Dr. Heiko Knospe Professor Fakultät IME
Niveau	Master
Semester im Jahr	Wintersemester
Dauer	Semester
Stunden im Selbststudium	78
ECTS	5
Dozenten	Prof. Dr. Heiko Knospe Professor Fakultät IME
Voraussetzungen	Voraussetzungen, Sicherheitsziele und Anwendung kryptographischer Verfahren: symmetrische Verschlüsselung, Hashverfahren, Message Authentication Codes, Erzeugung von Pseudozufallszahlen, asymmetrische Verschlüsselung, Signaturen, Schlüsselvereinbarung.
Unterrichtssprache	englisch
separate Abschlussprüfung	Ja

Abschlussprüfung

Details

Klausur

Mindeststandard

Bestehen der Klausur

^ Vorlesung / Übungen

Lernziele

Kenntnisse

Introduction to IT Security

- Standards and Guidelines
 - Taxonomy
 - Security Objectives, Vulnerabilities, Threats, Risk, Attacks, Security Controls
-

Authentication and Key Establishment

- Authentication Protocols
 - Key Exchange
 - Kerberos
 - Public Key Infrastructures
 - Passwords and their Vulnerabilities
 - Security Token
-

Access Control

- Authentication, Authorization, Auditing
 - Discretionary and Mandatory Access Control
 - Access Matrix, Unix ACL
 - Role-Based Access Control
 - Multi-Level Security, Bell-LaPadula Model
-

Network Security

- Threat Model
 - LAN and WLAN Security
 - IP Security, IPsec
 - TCP Security, TLS, SSH
 - Virtual Private Networks
 - IDS and IPS
 - Firewalls and UTM
 - DNS Security
-

Software Security

- Safety and Security
 - Software Vulnerabilities
 - Web Security
-

Security Management

- Information Security Management System

- Security Standards ISO 27001, ISO 27002, BSI Grundschutz
- Privacy Regulations

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Vorlesung	2
Übungen (ganzer Kurs)	1
Übungen (geteilter Kurs)	0
Tutorium (freiwillig)	0

Separate Prüfung

keine

^ Praktikum

Lernziele

Fertigkeiten

- Generation of key pairs, certificates and setting up a public-key infrastructure (PKI).
- Implementation of a secure socket connection and analysis of a TLS handshake.
- Implementation and analysis of a VPN.
- Penetration testing of web applications using open source tools.
- Perform SQL injection, XSS and CSRF attacks against test systems.
- Reconnaissance, exploitation and infiltration in a lab environment.
- Interpret DNS and HTTP data to analyze an attack.

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Praktikum	1
Tutorium (freiwillig)	0

Separate Prüfung

Prüfungstyp

praxisnahes Szenario bearbeiten (z.B. im Praktikum)

Details

Testat und individuelle Lernstandsrückmeldung

Mindeststandard

Erfolgreiche Bearbeitung der aller Praktikumsaufgaben