Technology
Arts Sciences
TH Köln

Lehrveranstaltung
ITS - IT-Sicherheit

Version: 2 | Letzte Änderung: 05.04.2022 18:44 | Entwurf: 0 | Status: vom verantwortlichen Dozent freigegeben

Allgemeine Informationen

Langname	IT-Sicherheit
Anerkennende LModule	ITS_BaET, ITS_BaTIN
Verantwortlich	Prof. Dr. Heiko Knospe Professor Fakultät IME
Niveau	Bachelor
Semester im Jahr	Sommersemester
Dauer	Semester
Stunden im Selbststudium	60
ECTS	5
Dozenten	
Voraussetzungen	- Programmier-Kenntnisse, insbesondere Java, C und Skriptsprachen. - Betriebssysteme-Kenntnisse, insbesondere Linux. - Datennetz-Kenntnisse, insbesondere TCP/IP. - Mathematik-Kenntnisse, insbesondere Mengen, Abbildungen, Restklassen, lineare Abbildungen.
Unterrichtssprache	deutsch, englisch bei Bedarf
separate Abschlussprüfung	Ja

Abschlussprüfung

Details

Klausur

Mindeststandard

Erfolgreicher Abschluss des Praktikums und Bestehen der Klausur

Prüfungstyp

Klausur

Vorlesung / Übungen

Lernziele

Kenntnisse

Grundlagen der IT-Sicherheit: Standards und Richtlinien, Taxonomie, Sicherheitsziele, Bedrohungen, Risiko, Angriffe, Maßnahmen.

Verfahren der Kryptographie: mathematische und algebraische Grundlagen, Definitionen von Sicherheit, historische Chiffren, symmetrische Verschlüsselung, Blockchiffren, Betriebsmodi, Stromchiffren, Hashverfahren, Message Authentication Codes, asymmetrische Verschlüsselung, RSA, Schlüsselvereinbarung, Diffie-Hellman, Signaturverfahren.

Authentifikation, Schlüsselvereinbarung und Zugriffskontrolle: Verfahren der Authentifikation, Passwörter, Schlüsselvereinbarung, Protokolle, öffentliche Schlüssel und Public-Key Infrastrukturen (PKI), Strategien der Zugriffskontrolle, Zugriffsmatrix, Unix ACL.

Netzwerksicherheit: TLS Protokoll.

Software- und Websicherheit: Grundlegende Prinzipien und Design sicherer Software, Schwachstellen, Angriffe gegen Webanwendungen.

Sicherheitsmanagement: Risikomanagement, Organisation des Sicherheitsprozesses, Sicherheitsstandards, insbesondere ISO 27000 Reihe und IT-Grundschutz, Datenschutz (Privacy), Gesetze, ethische Aspekte.

Aufwand Präsenzlehre

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

Separate Prüfung

keine

Praktikum

Lernziele

Fertigkeiten

- Java Implementierung der AES Verschlüsselung und Entschlüsselung von Files.
- Einsatz unterschiedlicher Betriebsmodi für Blockchiffren.
- Statistische Analyse eines AES Chiffretextes.
- Erzeugung von Schlüsselpaaren, Zertifikaten und Aufbau einer Public-Key Infrastruktur mit Open Source Software.
- Installation und Härtung eines Linux-Systems.
- Aufbau eines sicheren Webservers.
- Angriffe gegen schwache Passwörter.
- Angriffe gegen Web-Applikationen (Testsystem).
- Einsatz von Software zur Erkennung und Analyse von Schwachstellen.

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 aller Praktikumsaufgaben