Technology
Arts Sciences
TH Köln

Lehrveranstaltungshandbuch 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
Gültig ab	Sommersemester 2022
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.

Literatur

C. Eckert, IT-Sicherheit, Oldenbourg Verlag

D. Gollmann, Computer Security, John Wiley & Sons

J. Schwenk, Sicherheit und Kryptographie im Internet, Springer Verlag

G. Schäfer, M. Roßberg, Netzsicherheit, dpunkt Verlag

W. Stallings, L. Brown, Computer Security: Principles and Practice, Pearson

N. Pohlmann, Cyber-Sicherheit, Springer Verlag

H. Knospe, A Course in Cryptography, American Mathematical Society

H. Kersten, G. Klett, J. Reuter, K.-W. Schröder, IT-Sicherheitsmanagement nach der neuen ISO 27001. Springer.

C. Paar, J. Pelzl, Kryptografie verständlich, Springer.

P. C. van Oorschot, Computer Security and the Internet, Springer.

Abschlussprüfung

Details	Klausur

Unterrichtssprache	deutsch, englisch bei Bedarf
separate Abschlussprüfung	Ja

Mindeststandard	Erfolgreicher Abschluss des Praktikums und Bestehen der Klausur
Prüfungstyp	Klausur

− Vorlesung / Übungen

Lernziele

Zieltyp	Beschreibung
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

Besondere Voraussetzungen

-

Begleitmaterial	undefined
Separate Prüfung	Nein

Übungen (ganzer Kurs)	1
Übungen (geteilter Kurs)	1
Tutorium (freiwillig)	0

− Praktikum

Lernziele

Zieltyp	Beschreibung
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

Besondere Voraussetzungen

-

Begleitmaterial	Online Kurs "Cybersecurity Essentials"
Separate Prüfung	Ja

Separate Prüfung

Prüfungstyp	praxisnahes Szenario bearbeiten (z.B. im Praktikum)
Details	Testat und individuelle Lernstandsrückmeldung
Mindeststandard	Erfolgreiche Bearbeitung aller Praktikumsaufgaben