

Modul

ITS - IT-Sicherheit

Bachelor Technische Informatik 2020

Version: 2 | Letzte Änderung: 05.04.2022 20:23 | Entwurf: 0 | Status: vom Modulverantwortlichen freigegeben | Verantwortlich: Knospe

^ Allgemeine Informationen

Anerkannte Lehrveranstaltungen	ITS_Knospe
Fachsemester	4
Dauer	1 Semester
ECTS	5
Zeugnistext (de)	IT-Sicherheit
Zeugnistext (en)	IT Security
Unterrichtssprache	deutsch oder englisch
abschließende Modulprüfung	Ja

Modulprüfung

Benotet	Ja
Frequenz	Jedes Semester

Prüfungskonzept

Schriftliche Prüfung (Klausur)

^ Allgemeine Informationen

Inhaltliche Voraussetzungen

PI1 - Praktische Informatik 1	-
PI2 - Praktische Informatik 2	-
NP - Netze und Protokolle	-
MA1 - Mathematik 1	-
MA2 - Mathematik 2	-

Kompetenzen

Kompetenz	Ausprägung
In Systemen denken	Vermittelte Kompetenzen
fachliche Probleme abstrahieren und formalisieren	Vermittelte Kompetenzen
Systeme analysieren	Vermittelte Kompetenzen
Systeme prüfen	Vermittelte Voraussetzungen für Kompetenzen
Informationen beschaffen und auswerten; Technische Zusammenhänge darstellen und erläutern	Vermittelte Kompetenzen
Typische Werkzeuge, Standards und Best Practices der industriellen Praxis kennen und einsetzen	Vermittelte Voraussetzungen für Kompetenzen
In vorhandene Systeme einarbeiten und vorhandene Komponenten sinnvoll nutzen	Vermittelte Voraussetzungen für Kompetenzen
Gesellschaftliche und ethische Grundwerte anwenden	Vermittelte Voraussetzungen für Kompetenzen

^ Vorlesung / Übungen

Exemplarische inhaltliche Operationalisierung

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, Schlüsselveinbarung, Diffie-Hellman, Signaturverfahren.

Authentifikation, Schlüsselveinbarung und Zugriffskontrolle: Verfahren der Authentifikation, Passwörter, Schlüsselveinbarung, 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.

Separate Prüfung

keine

^ Praktikum

Exemplarische inhaltliche Operationalisierung

- 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.

Separate Prüfung

Benotet	Nein
Frequenz	Einmal im Jahr
Voraussetzung für Teilnahme an Modulprüfung	Ja

Prüfungskonzept

