Technology
Arts Sciences
TH Köln

Modulhandbuch 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
Gültig ab	Sommersemester 2022
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
Konzept	Schriftliche Prüfung (Klausur)
Frequenz	Jedes Semester

− Allgemeine Informationen

Inhaltliche Voraussetzungen

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

Handlungsfelder

- Systeme zur Verarbeitung, Übertragung und Speicherung von Informationen für technische Anwendungen planen, realisieren und integrieren
- Anforderungen, Konzepte und Systeme analysieren und bewerten
- Informationstechnische Systeme und Prozesse organisieren und betreiben
- Mit Auftraggebern, Anwendern, gesellschaftlichem Umfeld und Teammitgliedern interagieren

Learning Outcomes

ID	Learning Outcome
LO1	Was: Das Modul vermittelt die grundlegenden Konzepte und Verfahren der IT-Sicherheit, die für die meisten IT-Systeme und Anwendungen eine wichtige Rolle spielen (K. 1). Die Studierenden lernen die Analyse von Systemen in Bezug auf Sicherheitsanforderungen (K. 2 und K. 4). Hierfür ist grundlegendes Verständnis von Sicherheitsbedrohungen und Angriffen notwendig (K. 7). Die Studierenden lernen die grundlegenden Verfahren und Standards der IT-Sicherheit (K. 9). Ethische Grundwerte spielen in diesem Zusammenhang eine wichtige Rolle (K. 14). Womit: Der Dozent/die Dozentin vermittelt Wissen und Basisfertigkeiten in der Vorlesung. In der Übung bearbeiten die Studierenden unter Anleitung Aufgaben. Im Praktikum werden konkrete Probleme und Fragestellungen der IT-Sicherheit bearbeitet. Wozu: Grundlegende Kenntnisse der IT-Sicherheit und der Cyber-Sicherheit werden in mehreren Moduln des Studiengangs benötigt und sind anerkannter und notwendiger Teil der Basisausbildung. Bei der Planung von Systemen für technische Anwendungen (HF 1), der Analyse und Bewertung von Anforderungen (HF2) sowie dem Betrieb von IT-Systemen (HF3) spielen Fragen der IT-Sicherheit heute eine wichtige Rolle. Dabei ist es notwendig mit Auftraggebern, Anwendern, dem gesellschaftlichem Umfeld und Teammitgliedern zu interagieren (HF4).

Kompetenzen

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

Vorlesung / Übungen

Typ	Vorlesung / Übungen
Separate Prüfung	Nein
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, 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.

Praktikum

Typ	Praktikum
Separate Prüfung	Ja

Separate Prüfung

Benotet	Nein
Frequenz	Einmal im Jahr
Voraussetzung für Teilnahme an Modulprüfung	Ja
Konzept	Individuelle Lernstandsrückmeldung und Testat

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.