Technology
Arts Sciences
TH Köln

Modulhandbuch ITS

IT-Sicherheit

Bachelor Elektrotechnik 2020

Version: 2 | Letzte Änderung: 05.04.2022 18:34 | Entwurf: 0 | Status: vom Modulverantwortlichen freigegeben | Verantwortlich: Knospe

− Allgemeine Informationen

Anerkannte Lehrveranstaltungen	ITS_Knospe
Gültig ab	Sommersemester 2022
Fachsemester	4
Modul ist Bestandteil der Studienschwerpunkte	SE - Smart Energy AU - Automatisierungstechnik IOT - Internet of Things
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

Forschung: Von Ansätzen der Grundlagenforschung bis hin zur Industrieforschung. Entwicklung: Algorithmen, Software, Verfahren , Geräte, Komponenten und Anlagen.

Qualitätskontrolle von Produkten und Prozessen, Mess- und Prüftechnologien, Zertifizierungsprozesse.

IT Administration, Projektcontrolling einschließlich Budget. Tätigkeiten in Verwaltung, Behörden und Ministerien.

Learning Outcomes

ID	Learning Outcome
LO1	Was: Das Modul vermittelt die grundlegenden Konzepte und Verfahren der IT-Sicherheit, die für viele IT-Systeme und Anwendungen eine wichtige Rolle spielen (K. 4). Die Studierenden lernen die Analyse von Systemen in Bezug auf Sicherheitsanforderungen (K. 7). Hierfür ist ein Verständnis von Sicherheitsbedrohungen und Angriffen notwendig. Die Studierenden lernen die grundlegenden Verfahren und Standards der IT-Sicherheit um Systeme zu entwerfen, zu realisieren und zu prüfen (K. 8, K. 9, K. 10). Ethische Grundwerte spielen in diesem Zusammenhang eine wichtige Rolle (K. 18), z.B. beim Umgang mit personenbezogenen Daten, 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 werden in mehreren Moduln des Studiengangs verwendet und sind anerkannter Teil der Basisausbildung in technischen Fächern (HF 1). Bei der Planung von Systemen für technische Anwendungen, der Analyse und Bewertung von Anforderungen sowie der Administration von IT-Systemen spielen Fragen der IT-Sicherheit heute eine wichtige Rolle (HF 5). Die Sicherheit von IT-Systemen ist Teil der Qualitätskontrolle und kann auch in Zertifizierungsprozessen von Bedeutung sein (HF 2).

Kompetenzen

Kompetenz	Ausprägung
Erkennen, Verstehen und analysieren technischer Zusammenhänge	diese Kompetenz wird vermittelt
Technische Systeme analysieren	Voraussetzungen für diese Kompetenz (Wissen,...) werden vermittelt
Technische Systeme entwerfen	Voraussetzungen für diese Kompetenz (Wissen,...) werden vermittelt
Technische Systeme realisieren	Voraussetzungen für diese Kompetenz (Wissen,...) werden vermittelt
Technische Systeme prüfen	diese Kompetenz wird 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.