

Modulhandbuch IS

IT Security

Master Technische Informatik 2020

Version: 5 | Letzte Änderung: 05.04.2022 17:33 | Entwurf: 0 | Status: vom Modulverantwortlichen freigegeben |
Verantwortlich: Knospe

– Allgemeine Informationen

Anerkannte Lehrveranstaltungen	<u>IS_Knospe</u>
---	------------------

Gültig ab	Wintersemester 2020/21
------------------	---------------------------

Dauer	1 Semester
--------------	------------

ECTS	5
-------------	---

Zeugnistext (de)	IT-Sicherheit
-------------------------	---------------

Zeugnistext (en)	IT Security
-------------------------	-------------

Unterrichtssprache	englisch
---------------------------	----------

abschließende Modulprüfung	Ja
---------------------------------------	----

Modulprüfung

Benotet	Ja
----------------	----

Konzept	Schriftliche Prüfung (Klausur)
----------------	--------------------------------

Frequenz	Jedes Semester
-----------------	----------------

– Allgemeine Informationen

Inhaltliche Voraussetzungen

KRY Voraussetzungen,
- Sicherheitsziele und Anwendung
Cryptography kryptographischer Verfahren:
Diskrete Strukturen,
Wahrscheinlichkeit,
Zahlentheorie und Algebra,
symmetrische Verschlüsselung,
Blockchiffen, Stromchiffen,
Hashverfahren, Message
Authentication Codes, Erzeugung
von Pseudozufallszahlen,
asymmetrische Verschlüsselung,
Digitale Signaturen,
Schlüsselvereinbarung, Hybride
Verschlüsselung, Elliptische-
Kurven-Kryptographie.

Handlungsfelder

Komplexe Rechner-, Kommunikations- und
Eingebettete Systeme sowie komplexe Software-
Systeme unter interdisziplinären Bedingungen
entwerfen, realisieren und bewerten

Wissenschaftlich arbeiten und wissenschaftliche
Erkenntnisse anwenden und erweitern

Learning Outcomes

ID	Learning Outcome
LO1	<p>Was: Das Modul vertieft zentrale Konzepte und Verfahren der IT-Sicherheit, die für den Entwurf, die Analyse und die Implementierung von informationstechnischen Systemen vor dem Hintergrund von diversen Sicherheitsbedrohungen eine wichtige Rolle spielen (K. 1). Die Studierenden lernen die Analyse von Systemen in Bezug auf Sicherheitsanforderungen. Die Studierenden beschaffen sich hierfür Informationen aus unterschiedlichen Quellen und wenden wissenschaftliche Methoden an (HF 2, K. 10). Ethische und gesellschaftliche Grundwerte spielen im Zusammenhang mit Angriffen gegen die Sicherheit von Daten und Systemen eine wichtige Rolle (K. 2).</p> <p>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 Informationssicherheit bearbeitet.</p> <p>Wozu: Im Profil Network and Security des Studiengangs werden vertiefte Kenntnisse der IT-Sicherheit und Cyber-Sicherheit benötigt. Sie sind ein anerkannter und notwendiger Teil der Qualifikation für Fach- und Führungsaufgaben in diesem Bereich. Bei der Entwicklung und dem Betrieb von informationstechnischen Systemen spielen Fragen der IT-Sicherheit heute eine wichtige Rolle (HF1).</p>

Kompetenzen

Kompetenz**Ausprägung**

Komplexe Systeme und
Prozesse analysieren,
modellieren, realisieren,
testen und bewerten

diese Kompetenz wird
vermittelt

Anerkannte Methoden
für wissenschaftliches
Arbeiten beherrschen

diese Kompetenz wird
vermittelt

Gesellschaftliche
Vertretbarkeit
technischer Lösungen
bewerten

diese Kompetenz wird
vermittelt

– Vorlesung / Übungen

Typ	Vorlesung / Übungen
Separate Prüfung	Nein
Exemplarische inhaltliche Operationalisierung	<p>Introduction to IT Security</p> <ul style="list-style-type: none">- Standards and Guidelines- Taxonomy- Security Objectives, Vulnerabilities, Threats, Risk, Attacks, Security Controls <p>Authentication and Key Establishment</p> <ul style="list-style-type: none">- Authentication Protocols- Key Exchange- Kerberos- Public Key Infrastructures- Passwords and their Vulnerabilities- Security Token <p>Access Control</p> <ul style="list-style-type: none">- Authentication, Authorization, Auditing- Discretionary and Mandatory Access Control- Access Matrix, Unix ACL- Role-Based Access Control- Multi-Level Security, Bell-LaPadula Model <p>Network Security</p> <ul style="list-style-type: none">- Threat Model- LAN and WLAN Security- IP Security, IPsec- TCP Security, TLS, SSH- Virtual Private Networks- IDS and IPS- Firewalls and UTM- DNS Security <p>Software Security</p> <ul style="list-style-type: none">- Safety and Security- Software Vulnerabilities- Web Security <p>Security Management</p> <ul style="list-style-type: none">- Information Security Management System- Security Standards ISO 27001, ISO 27002, BSI Grundschutz- Privacy Regulations

– Praktikum

Typ	Praktikum
------------	-----------

Separate Prüfung	Ja
-------------------------	----

Separate Prüfung	
-------------------------	--

Benotet	Nein
----------------	------

Frequenz	Einmal im Jahr
-----------------	----------------

Exemplarische inhaltliche Operationalisierung

- Generation of key pairs, certificates and setting up a public-key infrastructure (PKI).
- Implementation of a secure socket connection and analysis of a TLS handshake.
- Implementation and analysis of a VPN.
- Penetration testing of web applications using open source tools.
- Perform SQL injection, XSS and CSRF attacks against test systems.
- Reconnaissance, exploitation and infiltration in a lab environment.
- Interpret DNS and HTTP data to analyze an attack.

Voraussetzung für Teilnahme an Modulprüfung

Konzept Individuelle Lernstandsrückmeldung und Testat