

AUSFÜLLHILFE: BEWEGEN SIE DEN MAUSZEIGER ÜBER DIE ÜBERSCHRIFTEN. AUSFÜHRliche HINWEISE: [LEITFADEN MODULBESCHREIBUNG](#)

IT-Sicherheit						
Kennnummer	Workload	Credits/LP	Studiensemester	Häufigkeit des Angebots	Dauer	
	90 h	3			1	
1	Lehrveranstaltungen		Sprache	Kontaktzeit	Selbststudium	geplante Gruppengröße
	IT-Sicherheit		deutsch	2 SWS / 22,5h	67,5 h	15
2	Lernergebnisse (learning outcomes) / Kompetenzen					
	<p>Nachdem das Modul erfolgreich absolviert wurde, können die Studierenden</p> <p>Wissen (1)</p> <ul style="list-style-type: none"> Terminologie und Grundkonzepte der IT-Sicherheit beschreiben <p>Verständnis (2)</p> <ul style="list-style-type: none"> die Bedeutung primärer Schutzziele für IT-Systeme verstehen Schwachstellen von IT-Systemen verstehen Bedrohungen und Angriffe gegen IT-Systeme verstehen Computer-forensische Analysen verstehen Schutzmaßnahmen für IT-Systeme verstehen <p>Anwendung (3)</p> <ul style="list-style-type: none"> Methoden der IT-Sicherheit anwenden und implementieren <p>Analyse (4)</p> <ul style="list-style-type: none"> Schutzziele hinsichtlich ihrer Anwendbarkeit für gegebene IT-Systemideen bzw. IT-Systeme analysieren gegebene IT-Systeme hinsichtlich ihrer Schwachstellen analysieren gegebene IT-Systemideen bzw. IT-Systeme hinsichtlich möglicher Bedrohungen und Angriffe analysieren geeignete Schutzmaßnahmen für gegebene IT-Systemideen bzw. IT-Systeme analysieren <p>Synthese (5)</p> <ul style="list-style-type: none"> geeignete Technologiena Auswahl und Entwurfsentscheidungen vor dem Hintergrund der Vereinbarkeit von anwendungsspezifischen und sicherheitsrelevanten Anforderungen treffen Sicherheitsarchitekturen für komplexe IT-Systeme entwerfen <p>Evaluation / Bewertung (6)</p> <ul style="list-style-type: none"> Sicherheit von Architekturen und bestehenden IT-Systemen bewerten 					
3	Inhalte					
	<ul style="list-style-type: none"> Schutzziele Schwachstellen, Bedrohungen und Angriffe Computer-Forensik Schutzmaßnahmen 					
4	Lehrformen					
	Vorlesung inklusive Präsenz-Übungen					

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.4			

5	Teilnahmevoraussetzungen <ul style="list-style-type: none"> • Grundlegende Programmierkenntnisse
6	Prüfungsformen <p>a) Prüfungsleistung 1K (70%) (Klausur) (3 LP insgesamt für alle Teilprüfungsleistungen dieser Lehrveranstaltung)</p> <p>a) Prüfungsleistung 1sbA (30%) (Praktische Arbeit)</p>
7	Verwendung des Moduls <p>Wahlmodul im Masterstudiengang Business Application Architectures</p>
8	Modulbeauftragte/r und hauptamtlich Lehrende <p>Tobias Straub, M.Sc.</p>
9	Literatur <ul style="list-style-type: none"> • Eckert, C: IT-Sicherheit: Konzepte - Verfahren – Protokolle, De Gruyter, 2018 • Poguntke, W: Basiswissen IT-Sicherheit, Springer Campus, 2017 • Kofler, M: Hacking & Security: Das umfassende Handbuch, Rheinwerk Computing, 2018

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.4			