

ITR - IT-Security, IT-Recht und Datenschutz

ITR - IT-Security, IT-Law and Data Privacy

Allgemeine Informationen	
Modulkürzel oder Nummer	ITR
Eindeutige Bezeichnung	ITSecITRData-01-BA-M
Modulverantwortlich(e)	Prof. Dr. Stark, Thorsten (thorsten.stark@haw-kiel.de)
Lehrperson(en)	Prof. Dr. Stark, Thorsten (thorsten.stark@haw-kiel.de)
Wird angeboten zum	Sommersemester 2025
Moduldauer	1 Fachsemester
Angebotsfrequenz	Regelmäßig
Angebotsturnus	In der Regel im Wintersemester
Lehrsprache	Deutsch
Empfohlen für internationale Studierende	Ja
Ist als Wahlmodul auch für andere Studiengänge freigegeben (ggf. Interdisziplinäres Modulangebot - IDL)	Nein

Studiengänge und Art des Moduls (gemäß Prüfungsordnung)
Studiengang: B.Sc. - WINF 7 Sem. - Wirtschaftsinformatik (7 Sem.) Modulart: Pflichtmodul Fachsemester: 5

Kompetenzen / Lernergebnisse
<i>Kompetenzbereiche: Wissen und Verstehen; Einsatz, Anwendung und Erzeugung von Wissen; Kommunikation und Kooperation; Wissenschaftliches Selbstverständnis/Professionalität.</i>
Die Studierenden verstehen die grundlegenden Aspekte des IT-Sicherheitsmanagements und des betrieblichen Kontinuitätsmanagements. Sie kennen die Grundkonzepte von Angreifermodellen und verstehen im Ansatz die Funktionsweise verschiedener Angriffstechniken und Schutzmaßnahmen. Sie verstehen die Notwendigkeit für und die Kernelemente von verschiedenen Ansätzen zur Sicherstellung der Betriebskontinuität im Ereignisfall.
Die Studierenden sind in der Lage, eigene Analysen zur IT-Sicherheit im betrieblichen Umfeld durchzuführen, und die Ergebnisse geeignet zu dokumentieren. Sie besitzen erste Kompetenzen zur Durchführung einer Risikobewertung und können den Aufwand einer vollständigen Risikobetrachtung im Rahmen eines betrieblichen Risikomanagements abschätzen.
Die Studierenden können selbst erarbeitete Inhalte mit Bezug zu IT-Sicherheit und Betriebskontinuität verständlich und überzeugend aufbereiten und präsentieren, sowie inhaltliche Aspekte sachgerecht und fachlich kompetent diskutieren.

Angaben zum Inhalt	
Lehrinhalte	<p>Grundlagen der klassischen IT-Sicherheit, Schutzziele, Angreifermodelle, Bedrohungen (Malware, Angriffstechniken), Schutz- und Gegenmaßnahmen, Risikomanagement nach IT-Grundschutz, Grundlagen der angewandten Kryptographie, Datenschutz-Grundlagen</p> <p>#angriffsvektoren #incidentmanagement #ethicalhacking #dsgvo #malware #itschutzmaßnahmen #risikomanagement #angriffsmethoden</p>
Literatur	<p>Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems Wiley; 2. edition (April 14, 2008) ISBN-13: 978-0470068526 Online verfügbar unter http://www.cl.cam.ac.uk/~rja14/book.html</p> <p>Matt Bishop: Computer Security – Art and Science Addison-Wesley Professional; 1. edition (December 12, 2002) ISBN-13: 978-0201440997</p> <p>Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C Wiley; 2. edition (November 2, 1995) ISBN-13: 978-0471128458</p>

Lehrformen der Lehrveranstaltungen	
Lehrform	SWS
Lehrvortrag + Übung	4

Arbeitsaufwand	
Anzahl der SWS	4 SWS
Leistungspunkte	5,00 Leistungspunkte
Präsenzzeit	48 Stunden
Selbststudium	102 Stunden

Modulprüfungsleistung	
Voraussetzung für die Teilnahme an der Prüfung gemäß PO	Keine
ITR - Präsentation	<p>Prüfungsform: Präsentation Dauer: 30 Minuten Gewichtung: 100% wird angerechnet gem. § 11 Absatz 2 PVO: Ja Benotet: Ja</p>

Sonstiges	
Sonstiges	Dieses Modul wird erstmals im Wintersemester 2024 / 2025 angeboten.