ITR - IT-Security, IT-Recht und Datenschutz

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

Allgemeine Informationen	
Modulkürzel oder Nummer	ITR
Eindeutige Bezeichnung	ITSecITRDatB-01-BA-M
Modulverantwortlich	Prof. Dr. Kürtz, Klaas Ole (klaas.o.kuertz@haw-kiel.de)
Lehrperson(en)	Prof. Dr. Kürtz, Klaas Ole (klaas.o.kuertz@haw-kiel.de) Prof. Dr. Stark, Thorsten (thorsten.stark@haw-kiel.de)
Wird angeboten zum	Wintersemester 2026/27
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
Kompetenzbereiche: Wissen und Verstehen; Einsatz, Anwendung und Erzeugung von Wissen; Kommunikation und Kooperation; Wissenschaftliches Selbstverständnis/Professionalität.
Die Studierenden verstehen die grundlegenden Aspekte des Managements der Cybersicherheit und der digitalen Resilienz. Sie kennen die Grundkonzepte von Angreifermodellen und verstehen im Ansatz die Funktionsweise verschiedener Angriffstechniken. Sie kennen Grundlagen der Kryptographie, ausgewählte Sicherheitsmechanismen, und Systematik von möglichen Schutzmaßnahmen. Sie verstehen die Notwendigkeit für und die Kernelemente von verschiedenen Ansätzen zur Sicherstellung der betrieblichen Kontinuität im Ereignisfall. Die Studierenden kennen grundsätzlich die von IT-Recht und Datenschutz betroffenen Themenfelder.
Die Studierenden können Ebenen der Cybersicherheit im Kontext von Unternehmen oder Organisationen anwenden, inklusive mathematisch-kryptographischer Grundlagen, technischer Maßnahmen, organisatorischer und strategischer Maßnahmen, Elementen menschlichen Verhaltens sowie rechtlichen Aspekten. Die Studierenden sind in der Lage, eigene Analysen zur Cybersicherheit im betrieblichen Umfeld durchzuführen und die Ergebnisse geeignet zu dokumentieren. Sie besitzen erste Kompetenzen zur Durchführung einer Risikobewertung.
Die Studierenden können Problemstellungen der Cybersicherheit und des IT-Rechts erörtern und diskutieren. Die Studierenden können selbst erarbeitete Inhalte mit Bezug zu Cybersicherheit, digitaler Resilienz und IT-Recht verständlich und überzeugend aufbereiten und präsentieren, sowie inhaltliche Aspekte sachgerecht und fachlich kompetent diskutieren. Sie können kompetent einschätzen, wann rechtliche Fragestellungen das Einbeziehen von Expert*innen erfordert.

Angaben zum Inhalt	
Lehrinhalte	Grundlagen der Cybersicherheit, Informationssicherheit, IT-Sicherheit, digitalen Resilienz Angreifermodelle und Bedrohungen, Angriffstechniken Schutzziele, Schutz- und Gegenmaßnahmen zur Sicherung von Daten, IT-Systemen und Organisationen Grundlagen der angewandten Kryptographie und des Risiko- und Krisenmanagements Grundlagen im IT-Recht inklusive Datenschutz #cybersicherheit #itsicherheit #digitaleresilienz #angriffsvektoren #angriffsmethoden #risikomanagement #dsgvo
Literatur	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 Matt Bishop: Computer Security – Art and Science Addison-Wesley Professional; 1. edition (December 12, 2002) ISBN-13: 978-0201440997 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C Wiley; 2. edition (November 2, 1995) ISBN-13: 978-0471128458

Lehrveranstaltungen

Pflicht-Lehrveranstaltung(en)

Für dieses Modul sind sämtliche in der folgenden Auflistung angegebenen Lehrveranstaltungen zu belegen.

ITRD - IT-Recht und Datenschutz - Seite: 6
ITS - IT-Security - Seite: 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 - Klausur	Prüfungsform: Klausur Dauer: 60 Minuten Gewichtung: 50% wird angerechnet gem. § 11 Absatz 2 PVO: Nein Benotet: Ja Anmerkung: IT-Security

ITR - Präsentation	Prüfungsform: Präsentation Dauer: 30 Minuten Gewichtung: 50% wird angerechnet gem. § 11 Absatz 2 PVO: Nein Benotet: Ja Anmerkung: IT-Recht und Datenschutz

Lehrveranstaltung: IT-Security

Allgemeine Informationen	
Veranstaltungsname	IT-Security IT-Security
Veranstaltungskürzel	ITS
Lehrperson(en)	Prof. Dr. Kürtz, Klaas Ole (klaas.o.kuertz@haw-kiel.de)
Angebotsfrequenz	Regelmäßig
Angebotsturnus	In der Regel im Wintersemester
Lehrsprache	Deutsch

Kompetenzen / Lernergebnisse
Kompetenzbereiche: Wissen und Verstehen; Einsatz, Anwendung und Erzeugung von Wissen; Kommunikation und Kooperation; Wissenschaftliches Selbstverständnis/Professionalität.
Die Studierenden verstehen die grundlegenden Aspekte des Managements der Cybersicherheit und der digitalen Resilienz. Sie kennen die Grundkonzepte von Angreifermodellen und verstehen im Ansatz die Funktionsweise verschiedener Angriffstechniken. Sie kennen Grundlagen der Kryptographie, ausgewählte Sicherheitsmechanismen, und Systematik von möglichen Schutzmaßnahmen. Sie verstehen die Notwendigkeit für und die Kernelemente von verschiedenen Ansätzen zur Sicherstellung der betrieblichen Kontinuität im Ereignisfall. Die Studierenden kennen grundsätzlich die von IT-Recht und Datenschutz betroffenen Themenfelder.
Die Studierenden können Ebenen der Cybersicherheit im Kontext von Unternehmen oder Organisationen anwenden, inklusive mathematisch-kryptographischer Grundlagen, technischer Maßnahmen, organisatorischer und strategischer Maßnahmen, Elementen menschlichen Verhaltens sowie rechtlichen Aspekten. Die Studierenden sind in der Lage, eigene Analysen zur Cybersicherheit im betrieblichen Umfeld durchzuführen und die Ergebnisse geeignet zu dokumentieren. Sie besitzen erste Kompetenzen zur Durchführung einer Risikobewertung.
Die Studierenden können Problemstellungen der Cybersicherheit und des IT-Rechts erörtern und diskutieren. Die Studierenden können selbst erarbeitete Inhalte mit Bezug zu Cybersicherheit, digitaler Resilienz und IT-Recht verständlich und überzeugend aufbereiten und präsentieren, sowie inhaltliche Aspekte sachgerecht und fachlich kompetent diskutieren. Sie können kompetent einschätzen, wann rechtliche Fragestellungen das Einbeziehen von Expert*innen erfordert.

Angaben zum Inhalt	
Lehrinhalte	Grundlagen der Cybersicherheit, Informationssicherheit, IT-Sicherheit, digitalen Resilienz Angreifermodelle und Bedrohungen, Angriffstechniken Schutzziele, Schutz- und Gegenmaßnahmen zur Sicherung von Daten, IT-Systemen und Organisationen Grundlagen der angewandten Kryptographie und des Risiko- und Krisenmanagements

Literatur	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 Matt Bishop: Computer Security – Art and Science Addison-Wesley Professional; 1. edition (December 12, 2002) ISBN-13: 978-0201440997 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C Wiley; 2. edition (November 2, 1995) ISBN-13: 978-0471128458

Lehrform der Lehrveranstaltung	
Lehrform	**SWS**
Lehrvortrag + Übung	2

Prüfungen	
Unbenotete Lehrveranstaltung	Nein

HAW Kiel
Hochschule für Angewandte Wissenschaften Kiel
Kiel University of Applied Sciences

Lehrveranstaltung: IT-Recht und Datenschutz

Allgemeine Informationen	
Veranstaltungsname	IT-Recht und Datenschutz IT-Law and Data Privacy
Veranstaltungskürzel	ITRD
Lehrperson(en)	Prof. Dr. Stark, Thorsten (thorsten.stark@haw-kiel.de)
Angebotsfrequenz	Regelmäßig
Angebotsturnus	In der Regel im Wintersemester
Lehrsprache	Deutsch

Kompetenzen / Lernergebnisse
Kompetenzbereiche: Wissen und Verstehen; Einsatz, Anwendung und Erzeugung von Wissen; Kommunikation und Kooperation; Wissenschaftliches Selbstverständnis/Professionalität.
Die Studierenden verstehen die grundlegenden Aspekte des Managements der Cybersicherheit und der digitalen Resilienz. Sie kennen die Grundkonzepte von Angreifermodellen und verstehen im Ansatz die Funktionsweise verschiedener Angriffstechniken. Sie kennen Grundlagen der Kryptographie, ausgewählte Sicherheitsmechanismen, und Systematik von möglichen Schutzmaßnahmen. Sie verstehen die Notwendigkeit für und die Kernelemente von verschiedenen Ansätzen zur Sicherstellung der betrieblichen Kontinuität im Ereignisfall. Die Studierenden kennen grundsätzlich die von IT-Recht und Datenschutz betroffenen Themenfelder.
Die Studierenden können Ebenen der Cybersicherheit im Kontext von Unternehmen oder Organisationen anwenden, inklusive mathematisch-kryptographischer Grundlagen, technischer Maßnahmen, organisatorischer und strategischer Maßnahmen, Elementen menschlichen Verhaltens sowie rechtlichen Aspekten. Die Studierenden sind in der Lage, eigene Analysen zur Cybersicherheit im betrieblichen Umfeld durchzuführen und die Ergebnisse geeignet zu dokumentieren. Sie besitzen erste Kompetenzen zur Durchführung einer Risikobewertung.
Die Studierenden können Problemstellungen der Cybersicherheit und des IT-Rechts erörtern und diskutieren. Die Studierenden können selbst erarbeitete Inhalte mit Bezug zu Cybersicherheit, digitaler Resilienz und IT-Recht verständlich und überzeugend aufbereiten und präsentieren, sowie inhaltliche Aspekte sachgerecht und fachlich kompetent diskutieren. Sie können kompetent einschätzen, wann rechtliche Fragestellungen das Einbeziehen von Expert*innen erfordert.

Angaben zum Inhalt	
Lehrinhalte	Grundlagen im IT-Recht inklusive Datenschutz, z.B. Abgrenzung Privatrecht / öffentliches Recht / Strafrecht; Vertragsschluss; EDV-Vertragsrecht, Softwareerstellung, Softwareüberlassung, Softwarewartung und Softwarepflege; Datenschutz; Jugendschutz; Domainrecht, Urheberrecht, Wettbewerbsrecht; Haftung im Offline- und Onlinebereich; Strafrecht; Internationale rechtliche Bezüge

Lehrform der Lehrveranstaltung	
Lehrform	**SWS**
Lehrvortrag + Übung	2

Prüfungen	
Unbenotete Lehrveranstaltung	Nein