

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	<p>Grundlagen der Cybersicherheit, Informationssicherheit, IT-Sicherheit, digitalen Resilienz</p> <p>Angreifermodelle und Bedrohungen, Angriffstechniken</p> <p>Schutzziele, Schutz- und Gegenmaßnahmen zur Sicherung von Daten, IT-Systemen und Organisationen</p> <p>Grundlagen der angewandten Kryptographie und des Risiko- und Krisenmanagements</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>
------------------	---

Lehrform der Lehrveranstaltung	
Lehrform	SWS
Lehrvortrag + Übung	2

Prüfungen	
Unbenotete Lehrveranstaltung	Nein