8.15 - IT-Security & Business Continuity Management

8.15 - IT-Security & Business Continuity Management

Allgemeine Informationen	
Modulkürzel oder Nummer	8.15
Eindeutige Bezeichnung	ITSecBusCont-01-BA-M
Modulverantwortlich(e)	Prof. Dr. Krauss, Christian (christian.krauss@haw-kiel.de)
Lehrperson(en)	Tams, Dennis (dennis.tams@haw-kiel.de)
Wird angeboten zum	Wintersemester 2023/24
Moduldauer	1 Fachsemester
Angebotsfrequenz	Regelmäßig
Angebotsturnus	In der Regel im Wintersemester
Lehrsprache	Deutsch
Empfohlen für internationale Studierende	Nein
Ist als Wahlmodul auch für andere Studiengänge freigegeben (ggf. Interdisziplinäres Modulangebot - IDL)	Nein

Studiengänge und Art des Moduls (gemäß Prüfungsordnung)
Studiengang: B.Sc. - WINF - Wirtschaftsinformatik (6 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 grundlegenen 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	Grundlagen der klassischen IT-Sicherheit, Schutzziele, Angreifermodelle, Bedrohungen (Malware, Angriffstechniken), Schutz- und Gegenmaßnahmen, Risikomanagement nach IT-Grundschutz, Grundlagen der angewandten Kryptographie, Datenschutz-Grundlagen #angriffsvektoren #incidentmanagement #ethicalhacking #dsgvo #malware #itschutzmaßnahmen #risikomanagement #angriffsmethoden
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

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
8.15 - Präsentation	Prüfungsform: Präsentation Dauer: 30 Minuten Gewichtung: 40% wird angerechnet gem. § 11 Absatz 2 PVO: Ja Benotet: Ja
8.15 - Klausur	Prüfungsform: Klausur Dauer: 90 Minuten Gewichtung: 60% wird angerechnet gem. § 11 Absatz 2 PVO: Nein Benotet: Ja