

8.15 - IT-Security & Business Continuity Management

8.15 - IT-Security & Business Continuity Management

General information	
Module Code	8.15
Unique Identifier	ITSecBusCont-01-BA-M
Module Leader(s)	Prof. Dr. Krauss, Christian (christian.krauss@haw-kiel.de)
Lecturer(s)	Tams, Dennis (dennis.tams@haw-kiel.de)
Offered in Semester	Wintersemester 2023/24
Module duration	1 Semester
Occurrence frequency	Regular
Module occurrence	In der Regel im Wintersemester
Language	Deutsch
Recommended for international students	No
Can be attended with different study programme	No

Curricular relevance (according to examination regulations)
Study Subject: B.Sc. - WINF - Wirtschaftsinformatik (6 Sem.) Module type: Pflichtmodul Semester: 5

Qualification outcome
<i>Areas of Competence: Knowledge and Understanding; Use, application and generation of knowledge; Communication and cooperation; Scientific self-understanding / professionalism.</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.

Content information	
Content	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

Literature	<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>
-------------------	---

Teaching formats of the courses	
Teaching format	SWS
Lehrvortrag + Übung	4

Workload	
Number of SWS	4 SWS
Credits	5,00 Credits
Contact hours	48 Hours
Self study	102 Hours

Module Examination	
Examination prerequisites according to exam regulations	None
8.15 - Präsentation	Method of Examination: Präsentation Duration: 30 Minutes Weighting: 40% wird angerechnet gem. § 11 Absatz 2 PVO: Yes Graded: Yes
8.15 - Klausur	Method of Examination: Klausur Duration: 90 Minutes Weighting: 60% wird angerechnet gem. § 11 Absatz 2 PVO: No Graded: Yes