

## 8.15 - IT-Security & Business Continuity Management

### 8.15 - IT-Security & Business Continuity Management

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

Studiengänge und Art des Moduls (gemäß Prüfungsordnung)
Studiengang: B.Sc. - WINF - Wirtschaftsinformatik (6 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.

<b>Angaben zum Inhalt</b>	
<b>Lehrinhalte</b>	<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>
<b>Literatur</b>	<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 <a href="http://www.cl.cam.ac.uk/~rja14/book.html">http://www.cl.cam.ac.uk/~rja14/book.html</a></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>

<b>Lehrformen der Lehrveranstaltungen</b>	
<b>Lehrform</b>	<b>SWS</b>
Lehrvortrag + Übung	4

<b>Arbeitsaufwand</b>	
<b>Anzahl der SWS</b>	4 SWS
<b>Leistungspunkte</b>	5,00 Leistungspunkte
<b>Präsenzzeit</b>	48 Stunden
<b>Selbststudium</b>	102 Stunden

<b>Modulprüfungsleistung</b>	
<b>Voraussetzung für die Teilnahme an der Prüfung gemäß PO</b>	Keine
<b>8.15 - Präsentation</b>	Prüfungsform: Präsentation Dauer: 30 Minuten Gewichtung: 40% wird angerechnet gem. § 11 Absatz 2 PVO: Ja Benotet: Ja
<b>8.15 - Klausur</b>	Prüfungsform: Klausur Dauer: 90 Minuten Gewichtung: 60% wird angerechnet gem. § 11 Absatz 2 PVO: Nein Benotet: Ja