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

# Course: IT-Security

| General information | |
|---|---|
| **Course Name** | IT-Security<br>IT-Security |
| **Course code** | ITS |
| **Lecturer(s)** | Prof. Dr. Kürtz, Klaas Ole (klaas.o.kuertz@haw-kiel.de) |
| **Occurrence frequency** | Regular |
| **Module occurrence** | In der Regel im Wintersemester |
| **Language** | Deutsch |

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

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

| | |
|---|---|
| **Literature** | Ross J. Anderson:<br>Security Engineering: A Guide to Building Dependable Distributed Systems<br>Wiley; 2. edition (April 14, 2008)<br>ISBN-13: 978-0470068526<br>Online verfügbar unter http://www.cl.cam.ac.uk/~rja14/book.html<br><br>Matt Bishop:<br>Computer Security – Art and Science<br>Addison-Wesley Professional; 1. edition (December 12, 2002)<br>ISBN-13: 978-0201440997<br><br>Bruce Schneier:<br>Applied Cryptography: Protocols, Algorithms, and Source Code in C<br>Wiley; 2. edition (November 2, 1995)<br>ISBN-13: 978-0471128458 |

| **Teaching format of this course** | |
|---|---|
| **Teaching format** | **SWS** |
| Lehrvortrag + Übung | 2 |

| **Examinations** | |
|---|---|
| **Ungraded Course Assessment** | No |