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

ITS - Einführung in die IT-Sicherheit
ITS - Introduction to IT Security

General information	
Module Code	ITS
Unique Identifier	EinfITSich-01-BA-M
Module Leader(s)	Prof. Dr. Aßmuth, Andreas (andreas.assmuth@haw-kiel.de)
Lecturer(s)	Prof. Dr. Aßmuth, Andreas (andreas.assmuth@haw-kiel.de)
Offered in Semester	Sommersemester 2025
Module duration	1 Semester
Occurrence frequency	Regular
Module occurrence	In der Regel im Sommersemester
Language	Deutsch
Recommended for international students	No
Can be attended with different study programme	No

Curricular relevance (according to examination regulations)
Study Subject: B.Eng. - E - Elektrotechnik (PO 2017, V3) Module type: Wahlmodul Semester: 6
Study Subject: B.Eng. - E - Elektrotechnik (PO 2023, V4) Module type: Wahlmodul Semester: 6
Study Subject: B.Eng. - Ming - Medieningenieur/-in (PO 2018, V1 + PO 2021, V2) Module type: Wahlmodul Semester: 4, 6
Study Subject: B.Sc. - INF - Informatik (PO 2021,V1) Module type: Pflichtmodul Semester: 4
Study Subject: B.Sc. - INI - Informationstechnologie (PO 2017, V1) Module type: Wahlmodul Semester: 4

Qualification outcome
Areas of Competence: Knowledge and Understanding; Use, application and generation of knowledge; Communication and cooperation; Scientific self-understanding / professionalism.
Die Studierenden kennen die Grundlagen der IT-Sicherheit (z. B. Bedrohungen und Schutzziele), ausgewählter Sicherheitsprotokolle und -mechanismen. Sie verfeinern ihre Kenntnisse über mathematische Methoden/Logik und wenden diese an. Sie kennen Grundbausteine der Kryptografie, die in Sicherheitsprotokollen zum Einsatz kommen. Durch das Nachstellen und die Analyse von Cyberangriffen vertiefen die Studierenden ihre Fähigkeit zur Abstraktion.
Die Studierenden können ausgewählte Konzepte zum Schutz einzelner Rechner und Computernetzwerke anwenden. Sie können Bedrohungen für einzelne Rechner sowie Computernetzwerke erkennen und analysieren. Sie können außerdem zur Gewährleistung von Schutzzielen (u. a. Vertraulichkeit, Authentizität oder Integrität) geeignete Sicherheitsmechanismen auswählen und einsetzen. Sie ergänzen ihre Fertigkeiten im Programmieren durch die Berücksichtigung von Security-Aspekten.

Die Studierenden lernen, Problemstellungen der IT-Sicherheit zu erörtern und zu diskutieren. Im Rahmen von praktischen Übungen vertiefen die Studierenden die Fähigkeit zur Arbeit in Teams. Durch Nutzung der englischsprachigen Literatur erlernen die Studierenden die entsprechenden international verwendeten Fachbegriffe.
Die Studierenden erlangen die Fähigkeit, selbstständig sicherheitsrelevante Problemstellungen zu identifizieren und verantwortungsvolle Entscheidungen zur Sicherung von IT-Systemen zu treffen. Sie entwickeln ein kritisches Verständnis für Sicherheitsrisiken und -mechanismen und lernen, ihre eigenen Analyse- und Lösungsstrategien regelmäßig zu reflektieren und zu verbessern. Durch gemeinsame praktische Übungen verbessern die Studierenden ihre Fähigkeiten zur Zusammenarbeit und zur Kommunikation technischer Inhalte, insbesondere bei der Diskussion von IT-Sicherheitsproblemen im Team.

Content information

Content	1 Bedrohungen und Risiken 2 Grundlagen der Kryptografie 3 Social Engineering 4 Endgeräte-Sicherheit: Angriffsflächen und Schutzmechanismen 5 Netzwerksicherheit 6 Penetration Testing und Ethical Hacking 7 IT-Sicherheit in der Anwendung
Literature	* Amberg, Eric und Daniel Schmid, "Hacking: Der umfassende Praxis-Guide", 3. Auflage, mitp, 2024. * Baucom, Michael, Moses Frost und Daniel Fernandez, "Gray Hat Hacking: The Ethical Hacker's Handbook", 6. Auflage, McGraw-Hill Education, 2022. * Eckert, Claudia, "IT-Sicherheit: Konzepte – Verfahren – Protokolle", 11. Auflage, De Gruyter Oldenbourg, 2023. * Hadnagy, Christopher, "Social Engineering: The Science of Human Hacking", 2. Auflage, 2018. * Jacobson, Douglas, "Introduction to Network Security", CRC, 2008. * Kofler, Michael und weitere, "Hacking u. Security: Das umfassende Handbuch", 3. Auflage, Rheinwerk Computing, 2022.

Teaching formats of the courses

Teaching format	SWS
Lehrvortrag	2
Labor	2

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
ITS - Laborprüfung	Method of Examination: Laborprüfung Weighting: 0% wird angerechnet gem. § 11 Absatz 2 PVO: Yes Graded: No Remark: Abgabe von mindestens 5 der 6 Laborberichte

ITS - Klausur	Method of Examination: Klausur Duration: 120 Minutes Weighting: 100% wird angerechnet gem. § 11 Absatz 2 PVO: No Graded: Yes Remark: Klausurrelevant sind außer den Inhalten der Vorlesungen auch die Inhalte der Laborübungen.

Miscellaneous	
Recommended Prerequisites	* Fortgeschrittene Mathematikkenntnisse, insbesondere Funktionen/Umkehrfunktionen, lineare Algebra, algebraische Strukturen, Zahlensysteme * Kenntnisse über den Aufbau und die Arbeitsweise von Computern * Kenntnisse über Computernetzwerke, insbesondere Ethernet, Internet-Protokoll, Adressierungsarten, Anwendungsprotokolle * grundlegende Programmierkenntnisse sowie Kenntnisse über Betriebssysteme