BI127 - Sicherheit in Netzwerken

BI127 - Network Security

Allgemeine Informationen	
Modulkürzel oder Nummer	BI127
Eindeutige Bezeichnung	SichNetzw-01-BA-M
Modulverantwortlich(e)	Prof. Dr. Aßmuth, Andreas (andreas.assmuth@haw-kiel.de) Caspar, Florian (florian.caspar@haw-kiel.de)
Lehrperson(en)	Caspar, Florian (florian.caspar@haw-kiel.de)
Wird angeboten zum	Sommersemester 2026
Moduldauer	1 Fachsemester
Angebotsfrequenz	Regelmäßig
Angebotsturnus	In der Regel jedes Semester
Lehrsprache	Deutsch
Empfohlen für internationale Studierende	Nein
Ist als Wahlmodul auch für andere Studiengänge freigegeben (ggf. Interdisziplinäres Modulangebot - IDL)	Ja

Studiengänge und Art des Moduls (gemäß Prüfungsordnung)
Studiengang: B.Eng. - Ming - Medieningenieur/-in (PO 2018, V1 + PO 2021, V2) Modulart: Wahlmodul Fachsemester: 4, 5, 6
Studiengang: B.Sc. - CS - Cybersicherheit Modulart: Wahlmodul Fachsemester: 7
Studiengang: B.Sc. - INF - Informatik (PO 2021,V1) Modulart: Wahlmodul Fachsemester: 4, 5, 6
Studiengang: B.Sc. - WINF 7 Sem. - Wirtschaftsinformatik (7 Sem.) Modulart: Wahlmodul Fachsemester: 4, 5, 6

Kompetenzen / Lernergebnisse
Kompetenzbereiche: Wissen und Verstehen; Einsatz, Anwendung und Erzeugung von Wissen; Kommunikation und Kooperation; Wissenschaftliches Selbstverständnis/Professionalität.
Die Studierenden können grundlegende Sicherheitstechniken und -protokolle verschiedener Netzwerkschichten – von der Anwendung bis hin zur Sicherungsschicht – benennen und erläutern. Sie können typische Bedrohungen und Angriffsvektoren in Netzwerken beschreiben und deren Relevanz für die IT-Sicherheit einordnen.
Die Studierenden können Sicherheitsmechanismen praktisch anwenden und sichere Systemarchitekturen entwerfen und konfigurieren. Sie sind in der Lage, Sicherheitslücken in Web-Applikationen zu identifizieren und zu vermeiden, Virtualisierungs- und Containertechnologien zur Erhöhung der IT-Sicherheit einzusetzen, Lieferkettenangriffe zu erkennen und zu analysieren sowie gängige Schutzmechanismen wie Firewalls, Web Application Firewalls oder Intrusion Prevention Systeme einzurichten und zu nutzen.

Die Studierenden können sicherheitsrelevante Problemstellungen erörtern und diskutieren. Sie sind in der Lage, Ergebnisse aus praktischen Übungen im Team abzustimmen und diese sowohl innerhalb von Arbeitsgruppen als auch im Plenum argumentativ zu präsentieren.
Die Studierenden können Werkzeuge zur sicheren Authentifizierung und Autorisierung einsetzen und kritisch reflektieren. Sie entwickeln ein Verständnis für die professionelle Bewertung und Auswahl sicherheitsrelevanter Maßnahmen und sind in der Lage, den Einsatz dieser Maßnahmen im Gesamtkontext der Netzwerksicherheit begründet zu beurteilen.

Angaben zum Inhalt

Lehrinhalte	- Sicherheit von Web-Applikationen - Erkennen, Ausnutzen und Vermeiden von Sicherheitslücken - Erhöhung der IT-Sicherheit durch Einsatz von Virtualisierung und Containerisierung - Durchführung und Erkennung von Lieferkettenangriffen - Einsatz von Packet-Filter-Firewalls, Web Application Firewalls und Intrusion Prevention Systemen - Praktischer Einsatz von Werkzeugen zur sicheren Authentifizierung und Autorisierung
Literatur	* 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.

Lehrformen der Lehrveranstaltungen

Lehrform	SWS
Labor	2
Lehrvortrag	2

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
BI127 - Laborprüfung	Prüfungsform: Laborprüfung Gewichtung: 0% wird angerechnet gem. § 11 Absatz 2 PVO: Ja Benotet: Nein Anmerkung: In der Prüfung wird bewertet, ob die Studierenden in der Lage sind, die in der Vorlesung gezeigten Techniken in der Praxis anzuwenden.

BI127 - Klausur	Prüfungsform: Klausur Gewichtung: 100% wird angerechnet gem. § 11 Absatz 2 PVO: Nein Benotet: Ja

Sonstiges	
Empfohlene Voraussetzungen	- Grundlegende Kenntnisse in Programmierung - Grundlegende Kenntnisse im Umgang mit Datenbankmanagementsystemen