Valid from 2024.HS

Module description: Cyber Security and Data Protection

Module Code	t.BA.MI.CSDS.23HS
ECTS Credits	4
Language of Instruction/Examination	German
Organizational Unit	InIT
Module Coordinator	Martin Ochoa Ronderos
Legal Framework	The module description is part of the legal basis in addition to the general academic regulations. It is binding. During the first week of the semester a written and communicated supplement can specify the module description in more detail.
Module Characteristic	Type 2a 4 consecutive lecture lessons per semester week and class
Module Description	This module provides students with fundamental knowledge in the areas of cyber security and data protection, particularly in the context of medical informatics. Students learn how to protect systems and data from attack and misuse, and how to develop and apply data protection policies and procedures.
Module Content	**This course introduces fundamental aspects of information security and data protection, with a special focus and examples from the healthcare sector. The theoretical lectures are complemented by practical exercises and group presentations. The following topics are covered in this lecture:** **Introduction, CIA (Confidentiality, Integrity, Availability), System and Attacker Models, Threat Modeling** **Access Control Policies** **Crypto 1: Symmetric Cryptography** **Crypto 2: Public Key Cryptography** **Hashes and Integrity, TLS (Transport Layer Security) and Certificates** **Network Security, Intrusion Detection** **Software Security, OWASP Top 10** **Operational Security, SIEMs (Security Information and Event Management), Threat Intelligence** **Data Protection and Privacy** **IoT Security in Healthcare**
Prerequisite Knowledge	

Module description: Cyber Security and Data Protection

Learning Objectives (Competences)

Students...	Competencies	Taxonomies
The participants understand how data confidentiality, authenticity, and integrity can be achieved during their transmission, processing, and storage, and what to pay attention to in this context.	F, M	K2
The participants are familiar with various approaches to analyze and test the security of a service, system, or product, and have practically applied specific methods in practical exercises (e.g., vulnerability scanners).	F	K2, K4
The participants understand what a data protection policy is and know how to design mechanisms for its enforcement.	F, M	K2, K3
The participants will gain an overview of the current threat situation or attack patterns, can name current examples, and have applied individual attack patterns themselves in practical exercises.	F	K2, K3
The participants can identify who wants to hack their systems and why ("Threat Landscape").	SE, F	K2

Performance Assessment

End-of-module exam	Assessment	Length (min.)	Weighting	Form
written exam	Grade	90	80	acc. to module agreement

Performance assessment during the semester	Assessment	Length (min.)	Weighting	Form
Labs and Presentations *Labs and Presentations*	Grade		20	acc. to module agreement

Classroom Attendance Requirement

None

Learning material

- Sean P. Murphy, Healthcare Information Security and Privacy, 2015
- William Stallings, Computer Security, 4th Edition, Pearson, 2017

Comments