**Gültig ab** 2024.HS

# Modulbezeichnung: Cyber Security und Datenschutz

| | |
|---|---|
| **Modulkürzel** | t.BA.MI.CSDS.23HS |
| **ECTS Credits** | 4 |
| **Unterrichts- und Prüfungssprache** | Deutsch |
| **Verantwortliche OE** | InIT |
| **Modulverantwortung** | Martin Ochoa Ronderos |
| **Rechtliche Grundlagen** | Die Modulbeschreibung ist neben Rahmenprüfungsordnung und Studienordnung Teil der Rechtsgrundlage. Sie ist verbindlich. Eine in der ersten Unterrichtswoche des Semesters schriftlich festgehaltene und kommunizierte Modulvereinbarung kann die Modulbeschreibung präzisieren. Die Modulvereinbarung ersetzt nicht die Modulbeschreibung. |
| **Modulausprägung** | Typ 2a<br><br>4 Lektionen Vorlesung aufeinanderfolgend pro Semesterwoche und Klasse |
| **Beschreibung des Moduls** | Dieses Modul vermittelt grundlegende Kenntnisse in den Bereichen Cyber Security und Datenschutz, insbesondere im Kontext der Medizininformatik. Die Studierenden lernen, wie sie Systeme und Daten vor Angriffen und Missbrauch schützen können und wie sie Datenschutzrichtlinien und -verfahren entwickeln und anwenden können. |
| **Inhalte des Moduls** | **In diesem Kurs werden grundlegende Aspekte der Informationssicherheit und des Datenschutzes vorgestellt, mit besonderem Schwerpunkt und Beispielen aus dem Gesundheitswesen. Die theoretischen Vorlesungen werden durch praktische Übungen und Gruppenpräsentationen begleitet. In dieser Vorlesung werden folgende Themen behandelt:**<br><br>**Einführung, CIA, System- und Angreifer Modelle, Bedrohungsmodellierung**<br><br>**Zugriffskontrollrichtlinien**<br><br>**Krypto 1: Symmetrische Krypto**<br><br>**Krypto 2: Öffentlicher Schlüssel**<br><br>**Hashes und Integrität, TLS und Zertifikate**<br><br>**Netzwerksicherheit, Einbruchserkennung**<br><br>**Softwaresicherheit, OWASP Top 10**<br><br>**Betriebssicherheit, SIEMs, Bedrohungsinformationen**<br><br>**Datenschutz und Privacy**<br><br>**IoT-Sicherheit im Gesundheitswesen** |
| **Vorkenntnisse** | |

# Modulbezeichnung: Cyber Security und Datenschutz

**Lernziele (Kompetenzen)**

| Die Studierenden... | Kompetenzen | Taxonomiestufen |
|---|---|---|
| Die Teilnehmenden verstehen, wie die Vertraulichkeit, Authentizität und Integrität von Daten während derer Übertragung, Verarbeitung und Speicherung erreicht werden kann und worauf dabeizu achten ist. | F, M | K2 |
| Die Teilnehmenden kennen verschiedene Ansätze um die Sicherheit eines Dienstes, Systems oder Produkts zu analysie-ren und zu testen und haben einzelne Verfahren im Praktikum praktisch angewandt (z.B. Schwachstellenscanner). | F | K2, K4 |
| Die Teilnehmer verstehen, was eine Datenschutzrichtlinie ist und wissen, wie sie Mechanismen zu deren Durchsetzung entwerfen können. | F, M | K2, K3 |
| Die Teilnehmenden können sich einen Überblick über die aktuelleBedrohungslage resp. aktuellen Angriffsmuster verschaffen, können aktuelle Beispiele benennen und haben einzelne Angriffsmuster im Praktikum selbst angewendet. | F | K2, K3 |
| Die Teilnehmenden können benennen, wer ihre Systeme knacken möchte und warum («Threat Landscape») | SE, F | K2 |

**Leistungsnachweis**

| Modulendprüfung | Bewertung | Dauer (Min.) | Gewichtung | Form |
|---|---|---|---|---|
| schriftliche Prüfung | Note | 90 | 80 | gem. Modulvereinbarung |

| Leistungsnachweise während dem Semester | Bewertung | Dauer (Min.) | Gewichtung | Form |
|---|---|---|---|---|
| Praktika und Presentationen<br>*Praktika und Presentationen* | Note | | 20 | gem. Modulvereinbarung |

**Präsenzverpflichtung im Kontaktstudium**

Keine

**Lernmaterialien**

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

**Bemerkungen**