**Gültig ab** 2026.HS

# Modulbezeichnung: IT Security

| | |
|---|---|
| **Modulkürzel** | t.BA.IT.ITS-EN.26HS |
| **ECTS Credits** | 4 |
| **Unterrichts- und Prüfungssprache** | Englisch |
| **Verantwortliche OE** | InIT |
| **Modulverantwortung** | Ariane Trammell |
| **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 3a<br><br>2 Lektionen Vorlesung pro Semesterwoche und Klasse + 2 Lektionen Praktikum pro Semesterwoche und Halbklasse |
| **Beschreibung des Moduls** | Enthält Grundlagen zu Entwicklung und Betrieb sicherer Systeme: Kryptographie (Secret- und Public-Key, Hashfunktionen, Signaturen/MAC), Sichere Protokolle, Authentifikation und Autorisierung sowie aktuelle Themen aus dem Bereich Cybersecurity. |
| **Inhalte des Moduls** | **Dieses Modul bietet eine Einführung in die Cybersecurity. Insbesondere werden folgende Themen behandelt:**<br><br>• - Einführung in die Kryptographie (Secret and Public Key Kryptographie, Hashfunktionen, Signaturen, Message Authentication Codes)<br>• - Zertifikate und Public Key Infrastructure<br>• - Sichere Protokolle (TLS, Quic, WPA2, etc.)<br>• - Mechanismen zum Absichern von Netzwerken (Network Access Control, Firewall, VPN, etc.)<br>• - Methoden zur Benutzerauthentisierung<br>• - Autorisierungskonzepte in Unix und Windows<br>• - Rechtliche Rahmenbedingungen mit Bezug auf Cybersecurity in der Schweiz<br>• - Einführung in Privacy Enhancing Technologies (PET)<br>• - Aktuelle Themen in den Bereichen Privacy und Cybersecurity |
| **Vorkenntnisse** | https://gpmpublic.zhaw.ch/GPMDocProdDPublic/2_Studium/2_02_Grundlagen_Studium/T_CL_Modulauspraegungen_SM2025.pdf |

# Modulbezeichnung: IT Security

**Lernziele (Kompetenzen)**

| Die Studierenden... | Kompetenzen | Taxonomiestufen |
|---|---|---|
| Die Studierenden kennen die Grundlagen der Kryptographie und können sie sicher anwenden. | M, F | K2, K3 |
| Die Studierenden kennen sichere Protokolle und können sie korrekt in eigenen Projekten einsetzen. | F, M | K2, K3, K4 |
| Die Studierenden kennen und verstehen die in Unix und Windows vorhandenen Mechanismen zur Autorisierung. | M, F | K2, K3 |
| Die Studierenden kennen verschiedene Mechanismen zur Authentifikation (Passwörter, Zertifikate, Token, ...) und können diese korrekt abwägen und einsetzen. | M, F | K2, K3, K4 |
| Die Studierenden kennen verschiedene Techniken zum Schutz von Netzwerken und kennen deren Eigenschaften und Limitationen. | F, M | K2, K3 |
| Die Studierenden können Privacy Enahncing Technologies an Fallbeispielen anwenden. | M | K3 |
| Die Studierenden sind mit den rechtlichen Rahmenbedingungen im Bereich IT-Sicherheit in der Schweiz vertraut. | M, F | K2, K3 |

**Leistungsnachweis**

| Modulendprüfung | Bewertung | Dauer (Min.) | Gewichtung | Sozialform | Szenario/Format |
|---|---|---|---|---|---|
| schriftliche Prüfung | | 90 | 80% | gem. Modulvereinbarung | |

| | Bewertung | Dauer (Min.) | Gewichtung | Sozialform | Szenario/Format |
|---|---|---|---|---|---|
| Praktikum<br>*In den Praktikums können Punkte gesammelt werden, welche zur Semesterendprüfung zählen. Dazu müssen die Praktika gelöst und dem Betreuer gezeigt werden.* | Note | 0 | 20% | gem. Modulvereinbarung | |

**Präsenzverpflichtung im Kontaktstudium**

Keine

**Lernmaterialien**

- Stallings, W. Computer Security (nicht verpflichtend). Pearson. ISBN 978-0134794105.