# ITS - Einführung in die IT-Sicherheit

# ITS - Introduction to IT Security

| Allgemeine Informationen | |
|---|---|
| **Modulkürzel oder Nummer** | ITS |
| **Eindeutige Bezeichnung** | EinfITSich-01-BA-M |
| **Modulverantwortlich(e)** | Prof. Dr. Aßmuth, Andreas (andreas.assmuth@haw-kiel.de) |
| **Lehrperson(en)** | Prof. Dr. Aßmuth, Andreas (andreas.assmuth@haw-kiel.de) |
| **Wird angeboten zum** | Sommersemester 2025 |
| **Moduldauer** | 1 Fachsemester |
| **Angebotsfrequenz** | Regelmäßig |
| **Angebotsturnus** | In der Regel im Sommersemester |
| **Lehrsprache** | Deutsch |
| **Empfohlen für internationale Studierende** | Nein |
| **Ist als Wahlmodul auch für andere Studiengänge freigegeben (ggf. Interdisziplinäres Modulangebot - IDL)** | Nein |

| Studiengänge und Art des Moduls (gemäß Prüfungsordnung) |
|---|
| Studiengang: B.Eng. - E - Elektrotechnik (PO 2017, V3)<br>Modulart: Wahlmodul<br>Fachsemester: 6 |
| Studiengang: B.Eng. - E - Elektrotechnik (PO 2023, V4)<br>Modulart: Wahlmodul<br>Fachsemester: 6 |
| Studiengang: B.Eng. - Ming - Medieningenieur/-in (PO 2018, V1 + PO 2021, V2)<br>Modulart: Wahlmodul<br>Fachsemester: 4, 6 |
| Studiengang: B.Sc. - INF - Informatik (PO 2021,V1)<br>Modulart: Pflichtmodul<br>Fachsemester: 4 |
| Studiengang: B.Sc. - INI - Informationstechnologie (PO 2017, V1)<br>Modulart: Wahlmodul<br>Fachsemester: 4 |

| Kompetenzen / Lernergebnisse |
|---|
| *Kompetenzbereiche: Wissen und Verstehen; Einsatz, Anwendung und Erzeugung von Wissen; Kommunikation und Kooperation; Wissenschaftliches Selbstverständnis/Professionalität.* |
| 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. |

## Angaben zum Inhalt

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

## Lehrformen der Lehrveranstaltungen

| Lehrform | SWS |
|---|---|
| Lehrvortrag | 2 |
| Labor | 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 |

| | |
|---|---|
| **ITS - Laborprüfung** | Prüfungsform: Laborprüfung<br>Gewichtung: 0%<br>wird angerechnet gem. § 11 Absatz 2 PVO: Ja<br>Benotet: Nein<br>Anmerkung: Abgabe von mindestens 5 der 6 Laborberichte |
| **ITS - Klausur** | Prüfungsform: Klausur<br>Dauer: 120 Minuten<br>Gewichtung: 100%<br>wird angerechnet gem. § 11 Absatz 2 PVO: Nein<br>Benotet: Ja<br>Anmerkung: Klausurrelevant sind außer den Inhalten der Vorlesungen auch die Inhalte der Laborübungen. |

| **Sonstiges** | |
|---|---|
| **Empfohlene Voraussetzungen** | * Fortgeschrittene Mathematikkenntnisse, insbesondere Funktionen/Umkehrfunktionen, lineare Algebra, algebraische Strukturen, Zahlensysteme<br>* Kenntnisse über den Aufbau und die Arbeitsweise von Computern<br>* Kenntnisse über Computernetzwerke, insbesondere Ethernet, Internet-Protokoll, Adressierungsarten, Anwendungsprotokolle<br>* grundlegende Programmierkenntnisse sowie Kenntnisse über Betriebssysteme |