Technische Hochschule Ingolstadt

Modulhandbuch

Cybersicherheit (SPO WS 22/23)

Bachelor

Fakultät Informatik

Studien- und Prüfungsordnung: WS 22/23

Stand: 30.04.2024

Inhalt

1 Übersicht 4

2 Einführung 5

2.1 Zielsetzung 6
2.2 Zulassungsvoraussetzungen 6
2.3 Zielgruppe 7
2.4 Studienaufbau 8
2.4.1 Erster Studienabschnitte 9
2.4.2 Zweiter Studienabschnitt 10
2.4.3 Fachwissenschaftliche Wahlpflichtmodule 12
2.5 Vorrückungsvoraussetzungen 13
2.6 Praktisches Studiensemester 13
2.7 Fachwissenschaftliche Wahlpflichtmodule der Virtuellen Hochschule Bayern (VHB) 14
2.8 Duales Studium 15
2.9 Konzeption 16

3 Qualifikationsprofil 17

3.1 Leitbild 18
3.2 Studienziele 19
3.2.1 Fachspezifische Kompetenzen des Studiengangs 19
3.2.2 Fachübergreifende Kompetenzen des Studiengangs 19
3.2.3 Prüfungskonzept des Studiengangs 21
3.2.4 Anwendungsbezug des Studiengangs 24
3.2.5 Beitrag einzelner Module zu den Studiengangzielen 25
3.3 Mögliche Berufsfelder 27

4 Modulbeschreibungen 28

4.1 Allgemeine Pflichtmodule 28
Einführungsprojekt 28
Grundlagen der Programmierung 1 30
Grundlagen der Programmierung 2 33
Einführung in die Informatik 1 35
Einführung in die Informatik 2 37
Grundlagen der IT-Sicherheit 39
Mathematik 1 41
Mathematik 2 43
Gesellschaftliche Verantwortung sowie Innere und Äußere Sicherheit 45
Software-Entwicklungsmethodik 47
Sichere Systeme 49
Angewandte Mathematik für IT-Sicherheit 51
Netzwerke 53
Softwaresicherheit & Security Testing 56
Software-Design, Software-Architektur und Datenbanken 58
Web-Technologien 60

Ethical Hacking Praktikum 62
Protokolle der Netzsicherheit 64
Security Architektur & Security Engineering 66
Projekt-, Qualitäts- und Risikomanagement 68
Recht für IT-Sicherheit und Datenschutz 70
Fachwissenschaftliches Seminar 72
Cloud-Architekturen und -Dienste 74
Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit 76
Incident Response und Netzwerkmonitoring 78
Sichere Netzwerkarchitekturen und Sicherheit vernetzter Anwendungen 80
Projekt 82
Grundlagen der Betriebswirtschaft und des Gründertums 84
Seminar Bachelorarbeit 86
Bachelorarbeit 88
Kommunikations- und Teamkompetenz 90
Praktikum (18 Wochen) 92
Nachbereitendes Praxisseminar 94

1 Übersicht

Dieses Dokument beschreibt den Bachelor-Studiengang „Cybersicherheit“. Insbesondere werden die Studienziele und Studieninhalte der einzelnen Pflichtmodule, der fachwissenschaftlichen Wahlpflichtmodule und der praxisbegleitenden Lehrveranstaltungen des Studiengangs sowie die zeitliche Aufteilung der Semesterwochenstunden je Fach und Studiensemester genannt.

Bei Mehrdeutigkeiten hat die übergeordnete Studien- und Prüfungsordnung Vorrang.

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für alle Geschlechter.

Die folgende Tabelle gibt einen Überblick über den Studiengang.

Name des Studiengangs	Cybersicherheit (Bachelor)
Studienart & Abschlussgrad	Grundständig, B.Sc. (Bachelor of Science), Vollzeit
Erstmaliges Startdatum	WS 2022/2023, jährlicher Start
Regelstudienzeit	7 Semester, 210 ECTS, 125 Semesterwochenstunden
Lage des Praxissemesters	5. Semester
Studienort	THI, Ingolstadt
Unterrichtssprache/n	Überwiegend deutsch (ab 2. Semester in jedem Semester mindestens eine englische Lehrveranstaltung)
Kooperation	ESG Elektroniksystem- und Logistik-GmbH
Zulassungsvoraussetzungen	Hochschulzugangsberechtigung
Kapazität	25 Studierende pro Studienjahr
Studiengangleiter	Prof. Dr. Hans-Joachim Hof E-Mail: hans-joachim.hof@thi.de Phone:+49 (0) 841 / 9348-2526
Studienfachberater	Prof. Dr. Michael Jarschel E-Mail: michael.jarschel@thi.de Phone:+49 (0) 841 / 9348-5184

Praktikumsbeauftragter	Prof. Dr. Bernd Hafenrichter E-Mail: bernd.hafenrichter@thi.de Phone: +49 (0) 841 / 9348-2522

2 Einführung

Als Teilgebiet der Informatik beschäftigt sich Cybersicherheit mit dem Schutz von Systemen und Informationen in all ihren Erscheinungsformen. Der Schutz umfasst insbesondere die Abwehr von mutwilligen, bösartigen Angriffen auf IT-Systeme oder Informationen. Im Gegensatz zur IT-Sicherheit betrachtet die Cybersicherheit den gesamten Cyberraum, der sämtliche mit dem globalen Internet verbundenen IT-Systeme und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen, Wissen und Intelligenz einschließlich der Akteure einschließt[1].

Der Bachelor-Studiengang Cybersicherheit konzentriert sich auf die technischen Aspekte der Cybersicherheit. Er bildet Studierende für den wachsenden Arbeitsmarkt auf diesem Gebiet aus. Dabei wird vom ersten Semester an besonders Wert auf die Entwicklung der Realisierungskompetenz der Studierenden sowie auf den Anwendungsbezug der Studieninhalte gelegt. Ziel des Studiengangs ist es, durch praxisorientierte Lehre eine auf der Grundlage wissenschaftlicher Erkenntnisse und Methoden beruhende Fach- und Realisierungskompetenz zu vermitteln, die zu einer eigenverantwortlichen Berufstätigkeit in allen Berufsfeldern befähigt, in denen der Schutz von IT-Systemen und Informationen eine Rolle spielt. Neben der Vermittlung von Fach- und Methodenkompetenz ist die Förderung der Persönlichkeitsentwicklung ein weiteres Ziel.

Mit Abschluss des Studiengangs kennen die Teilnehmer die wichtigsten Konzepte, Methoden und Techniken der Informatik und der Cybersicherheit und sind in der Lage, sie adäquat anzuwenden, um die Digitalisierung souverän zu gestalten (Digitale Souveränität). Die Absolventen können Sicherheitskonzepte für neue Systeme erstellen, Systeme auf IT-Sicherheit testen und Systeme im Betrieb sicher halten. Die Teilnehmer kennen und verstehen die nationale Sicherheits-Infrastruktur im Kontext der inneren, äußeren und öffentlichen Sicherheit und können die damit einhergehenden Verfahren und Gesetzgebungen anwenden.

[1] Definition Cybersicherheit und Cyberraum frei nach Norbert Pohlmann, Glossar Cybersicherheit

2.1 Zielsetzung

Bedingt durch die zunehmende Digitalisierung aller Lebensbereiche durchdringt Informationstechnologie schon heute unseren gesamten Alltag und unsere gesamte Gesellschaft – dieser Trend wird sich sicher auch in Zukunft fortsetzen. Mit den Effizienzgewinnen durch die Digitalisierung geht jedoch eine größere Verwundbarkeit durch Cyberangriffe einher. Es ist zu beobachten, dass sich die Angreifer zunehmend professionalisieren, seien es einfache Cyberkriminelle, Cyberspione oder auch staatliche Akteure. Für Unternehmen stellt sich nicht mehr die Frage ob, sondern wie Systeme zu schützen sind.

Ziel des Bachelorstudiengangs Cybersicherheit ist, durch praxisorientierte Lehre eine auf der Grundlage wissenschaftlicher Erkenntnisse und Methoden beruhende Fachkompetenz im Bereich Cybersicherheit zu vermitteln, die zu einer eigenverantwortlichen Berufstätigkeit mit dem Ziel des Schutzes von IT-Systemen befähigt. Neben der Vermittlung von Fach- und Methodenkompetenz ist die Förderung der Persönlichkeitsentwicklung ein weiteres Ziel.

Die Absolventen sollen nach ihrem Studium in der Lage sein, die wichtigsten Konzepte, Methoden und Techniken der Informatik und der Cybersicherheit adäquat anzuwenden, um die Digitalisierung souverän zu gestalten. Hierzu zählen beispielsweise die Erstellung von Sicherheitskonzepten für neue IT-Systeme, das Testen von IT-Systemen auf IT-Sicherheit und die Aufrechterhaltung des Sicherheitsniveaus von IT-Systemen im Betrieb. Das abgeschlossene Bachelorstudium bietet auch die Grundlage für eine wissenschaftliche Weiterqualifizierung in einem sich anschließenden Masterstudium.

2.2 Zulassungsvoraussetzungen

Für den Bachelorstudiengang müssen die allgemeinen Zulassungsvoraussetzungen für ein Studium an Hochschulen für angewandte Wissenschaften erfüllt sein.

Die verbindlichen Regelungen für diesen Studienplan sind zu finden in:

- Studien- und Prüfungsordnung für den Bachelorstudiengang Cybersicherheit in der Fassung vom 13.12.2021 ab WS 2022/23
- Allgemeine Prüfungsordnung (APO) der Technischen Hochschule Ingolstadt
- Immatrikulationssatzung der Technischen Hochschule Ingolstadt.

Der Studienablauf ist von den einschlägigen Bestimmungen der Studien- und Prüfungsordnung beeinflusst.

2.3 Zielgruppe

Der Studiengang richtet sich an:

- technisch interessierte Studienbewerber (grundständiger Bachelor), die einen Beruf oder eine Forschungskarriere im Bereich Cybersicherheit im privaten oder öffentlichen Sektor anstreben.
- Studienbewerber mit systembezogener Denkweise, gutem Abstraktionsvermögen und einem Grundverständnis von Mathematik.
- Studienbewerber, welche die erforderlichen Kompetenzen zum digital souveränen Handeln erwerben wollen und diese im privaten und öffentlichen Sektor (z.B. Gesundheitssystem) oder zur Wahrung der nationalen Souveränität oder der freiheitlich-demokratischen Grundordnung einsetzen wollen.
- Studienbewerber, die Interesse haben, sichere Systeme und Anwendungen zu planen, zu betreiben und die Entwicklung zu begleiten.
- Studienbewerber, welche die erforderlichen Kompetenzen zur Beurteilung der IT-Sicherheit durch praktische Tests erwerben wollen (Whitehat Hacking, Penetration Testing, Vulnerability Assessment).
- Studienbewerber, welche die erforderlichen Kompetenzen zur Nachverfolgung und Verhinderung von Angriffen auf Systemen sowie IT-Forensik erlernen wollen.

2.4 Studienaufbau

Die Regelstudienzeit für die Bachelor-Studiengänge umfasst sieben Semester. Die Studiengänge gliedern sich in zwei Studienabschnitte. Der erste Studienabschnitt umfasst zwei theoretische Studiensemester. Der zweite Studienabschnitt beinhaltet vier theoretische Semester und ein praktisches Semester, welches als 5. Studiensemester geführt wird.

Das folgende Schaubild bildet den Studienverlauf grafisch ab.

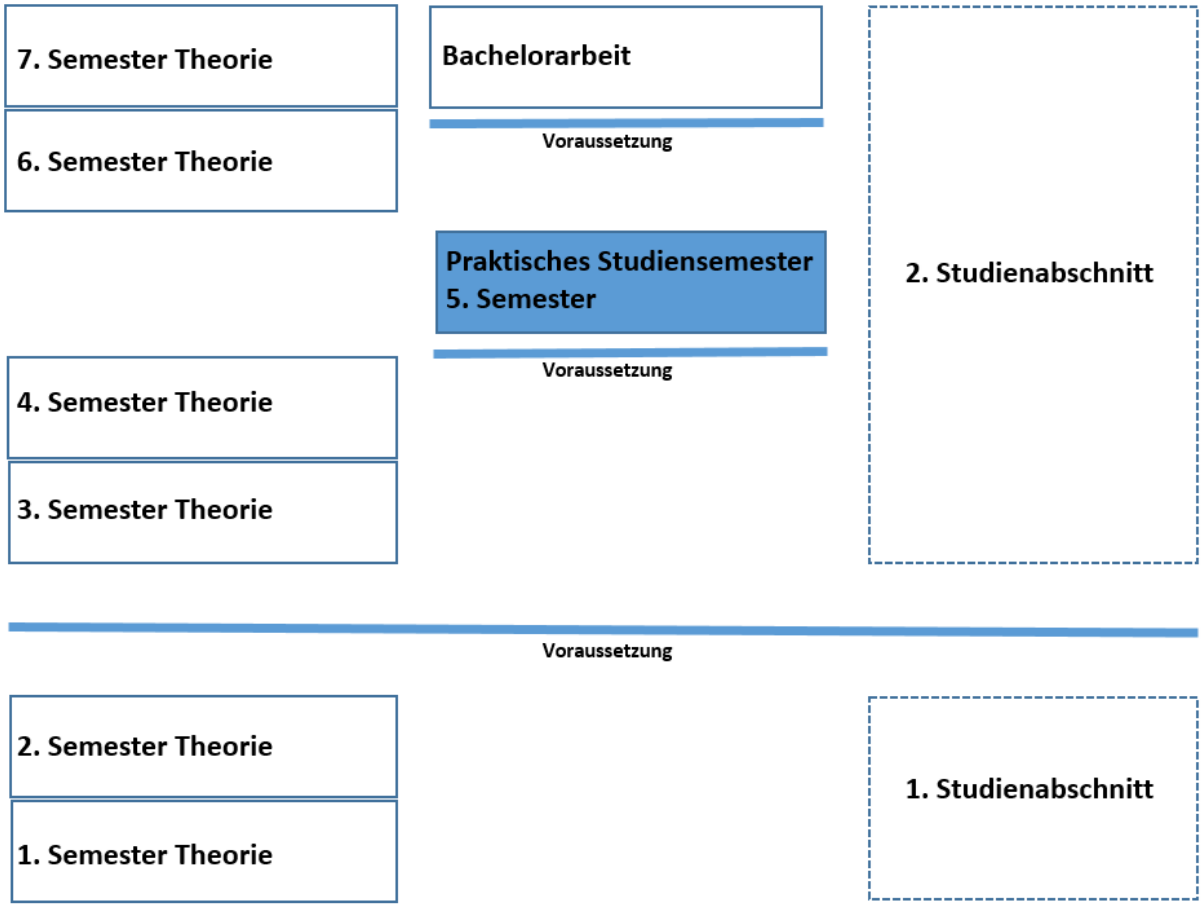


Abbildung 1 Aufbau des Studiums

Die Master-Studiengänge werden als Vollzeitstudium angeboten. Die Regelstudienzeit beträgt drei theoretische Studiensemester, wobei das dritte Semester der Anfertigung der Masterarbeit dient.

2.4.1 Erster Studienabschnitte

Der erste Studienabschnitt umfasst zwei theoretische Semester.

Modul	Nr.	Fach	Aufteilung nach Semestern			
			1. Sem	2. Sem	SWS	CP
Einführungsprojekt	1	Einführungsprojekt	LN		2	2
Grundlagen der Programmierung 1	2.1	Grundlagen der Programmierung 1	schrP		4	7
	2.2	Praktikum Grundlagen der Programmierung 1	LN		2	
Grundlagen der Programmierung 2	3.1	Grundlagen der Programmierung 2		schrP	4	7
	3.2	Praktikum Grundlagen der Programmierung 2		LN	2	
Einführung in die Informatik 1	4	Einführung in die Informatik 1	schrP		4	5
Einführung in die Informatik 2	5.1	Einführung in die Informatik 2		schrP	4	7
	5.2	Praktikum Einführung in die Informatik 2		LN	2	
Grundlagen der IT-Sicherheit	6	Grundlagen der IT-Sicherheit	schrP		4	5
Mathematik 1	7.1	Mathematik 1	schrP		4	6
	7.2	Übung zu Mathematik 1			1	
Mathematik 2	8.1	Mathematik 2		schrP	4	6
	8.2	Übung zu Mathematik 2			1	
Gesellschaftliche Verantwortung sowie Innere und Äußere Sicherheit	9	Gesellschaftliche Verantwortung sowie Innere und Äußere Sicherheit	schrP		4	5
Software-Entwicklungsmethodik	10	Software-Entwicklungsmethodik		schrP	4	5
Sichere Systeme	11	Sichere Systeme		schrP	4	5
Summe					**50**	**60**

Legende:

SWS	Semesterwochenstunden
CP	Leistungspunkte nach European Credit Transfer System (ECTS)
schrP	schriftliche Prüfung
LN	studienbegleitender Leistungsnachweis

Für Studien- und Prüfungsleistungen, die in mehreren Teilen oder in Fächern mit begleitenden Praktika zu erbringen sind, gelten ggf. Voraussetzungen, die in der Anlage zur SPO bzw. in den folgenden Modulbeschreibungen geregelt sind.

2.4.2 Zweiter Studienabschnitt

Der zweite Studienabschnitt beginnt ab dem dritten Semester und umfasst 4 theoretische Semester und ein Praxissemester.

Semester 3-5

Modul	Nr.	Fach	Aufteilung nach Semestern				
			3. Sem	4. Sem	5. Sem	SWS	CP
Angewandte Mathematik für IT-Sicherheit	12.1	Angewandte Mathematik für IT-Sicherheit	schrP			4	6
	12.2	Übung zu Angewandte Mathematik für IT-Sicherheit				1	
Netzwerke	13.1	Netzwerke	schrP			4	7
	13.2	Praktikum Netzwerke	LN			2	
Softwaresicherheit & Security Testing	14	Softwaresicherheit & Security Testing	schrP			4	5
Software-Design, Software-Architektur und Datenbanken	15.1	Software-Design, Software-Architektur und Datenbanken	schrP			4	7
	15.2	Praktikum Software-Design, Software-Architektur und Datenbanken				2	
Web-Technologien	16	Web-Technologien	schrP			4	5
Ethical Hacking Praktikum	17	Ethical Hacking Praktikum		LN		4	5
Protokolle der Netzsicherheit	18	Protokolle der Netzsicherheit		schrP		4	5
Security Architektur & Security Engineering	19.1	Security Architektur & Security Engineering		schrP		4	7
	19.2	Praktikum zu Security Architektur & Security Engineering		LN		2	
Projekt-, Qualitäts- und Risikomanagement	20	Projekt-, Qualitäts- und Risikomanagement		schrP		4	5
Fachwissenschaftliches Seminar	22	Fachwissenschaftliches Seminar		SA		2	3
Cloud-Architekturen und -Dienste	23	Cloud-Architekturen und -Dienste		schrP		4	5
Praktisches Studiensemester	31	Kommunikations- und Teamkompetenz			LN	1	2
	32	Praktikum (18 Wochen)			PrB		26
	33	Nachbereitendes Praxisseminar			LN	1	2
Summe						**51**	**90**

Legende:

SWS	Semesterwochenstunden
CP	Leistungspunkte nach European Credit Transfer System (ECTS)
schrP	schriftliche Prüfung
SA	Seminararbeit
LN	studienbegleitender Leistungsnachweis
PrB	Praktikumsbericht

Für Studien- und Prüfungsleistungen, die in mehreren Teilen oder in Fächern mit begleitenden Praktika zu erbringen sind, gelten ggf. Voraussetzungen, die in der Anlage zur SPO bzw. in den folgenden Modulbeschreibungen geregelt sind.

Semester 6-7

Modul	Nr.	Fach	Aufteilung nach Semestern			
			6. Sem	7. Sem	SWS	CP
Recht für IT-Sicherheit und Datenschutz	21	Recht für IT-Sicherheit und Datenschutz	schrP		2	3
Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit	24.1	Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit	schrP		4	7
	24.2	Praktikum Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit	LN		2	
Incident Response und Netzwerkmonitoring	25	Incident Response und Netzwerkmonitoring	schrP		4	5
Sichere Netzwerkarchitekturen und Sicherheit vernetzter Anwendungen	26	Sichere Netzwerkarchitekturen und Sicherheit vernetzter Anwendungen	schrP		4	5
Projekt	27	Projekt	Proj		4	5
Grundlagen der Betriebswirtschaft und des Gründertums	28	Grundlagen der Betriebswirtschaft und des Gründertums	schrP		4	5
Fachwissenschaftliche Wahlpflichtfächer	31.1	Fachwissenschaftliches Wahlpflichtfach 1		LN	4	5
	31.2	Fachwissenschaftliches Wahlpflichtfach 2		LN	4	5
	31.3	Fachwissenschaftliches Wahlpflichtfach 3		LN	4	5
Bachelorarbeit	30.1	Seminar Bachelorarbeit		LN	2	3
	30.2	Bachelorarbeit		BA		12
Summe					**38**	**60**

Legende:

SWS	Semesterwochenstunden
CP	Leistungspunkte nach European Credit Transfer System (ECTS)
schrP	schriftliche Prüfung
LN	studienbegleitender Leistungsnachweis
BA	Bachelorarbeit
Proj	Projekt

2.4.3 Fachwissenschaftliche Wahlpflichtmodule

Im 7. Semester sind regulär fachwissenschaftliche Wahlpflichtmodule (FW-Module) zu belegen.

Am Ende des vorausgehenden Semesters erfolgt die Einschreibung für die FW-Module (online über Moodle), um die Teilnehmerzahl zu ermitteln. Die einzelnen FW-Module können nur bei ausreichender Teilnehmerzahl angeboten werden.

Das Angebot an FW-Modulen wird für jedes Semester neu erstellt, je nach Verfügbarkeit der Dozenten bzw. Lehrbeauftragten aus der Industrie. Bei Interesse können nach Rücksprache mit dem Studiengangleiter auch geeignete Fächer anderer Studiengänge als FW-Fächer gewählt werden. Ein Anspruch darauf besteht nicht. Melden Sie sich dazu bitte in den ersten beiden Wochen des Semesters beim Studiengangleiter.

2.5 Vorrückungsvoraussetzungen

Um sicherzustellen, dass die für das Verständnis der einzelnen Studienabschnitte erforderlichen Kenntnisse vorhanden sind, gibt es mehrere Vorrückungsvoraussetzungen. Bei Nichterfüllen dieser Voraussetzungen entsteht meist eine Verzögerung im Studienfortschritt, die zum Füllen der jeweiligen Lücken genutzt werden soll. Um die Gesamtdauer des Studiums im Rahmen zu halten, sind zusätzlich einige Fristen zu beachten. Einen Überblick über diese Voraussetzungen und Fristen gibt die nachfolgende Aufstellung:

- Zum Eintritt in das dritte Studiensemester ist nur berechtigt, wer mindestens 42 ECTS-Leistungspunkte aus den Modulen des ersten Studienabschnittes erbracht hat.
- Zum Eintritt in das Praktikum als Teil des praktischen Studiensemesters ist nur berechtigt, wer in allen Prüfungen und bestehenserheblichen studienbegleitenden Leistungsnachweisen des ersten Studienabschnittes mindestens die Note „ausreichend“ erzielt hat sowie mindestens 20 ECTS-Leistungspunkte aus den Pflichtmodulen des zweiten Studienabschnittes erbracht hat.
- Voraussetzung für die Ausgabe der Bachelorarbeit ist die erfolgreiche Ableistung des praktischen Studiensemesters. Der früheste Ausgabezeitpunkt der Bachelorarbeit erfolgt, ausgehend von der Regelstudienzeit, frühestens zu Beginn des vorletzten Studiensemesters.

Die verbindlichen Regelungen sind im Wortlaut zu finden in der Studien- und Prüfungsordnung für den Bachelorstudiengang Cybersicherheit in der Fassung vom 13.12.2021 ab WS 2022/23 und in der Allgemeinen Prüfungsordnung (APO) der Technischen Hochschule Ingolstadt.

2.6 Praktisches Studiensemester

Das Praxissemester ist während des Studiums für alle Studierenden zu durchlaufen. Es wird in Unternehmen aus Industrie, Mittelstand und öffentlicher Verwaltung durchgeführt.

Das praktische Studiensemester des zweiten Studienabschnitts umfasst einen Zeitraum von 20 Wochen und wird durch drei Lehrveranstaltungen an der Hochschule begleitet, von denen eine vor (Vorbereitendes Praxisseminar - PLV1) und zwei nach der Praxisphase (Nachbereitendes Praxisseminar - PLV2, Informations- und Medienkompetenz - PLV3) stattfinden.

Begleitend zum Praxissemester ist ein Praktikumsbericht anzufertigen. Die Anforderungen an den Praktikumsbericht sind in der Anlage zur SPO aufgeführt.

2.7 Fachwissenschaftliche Wahlpflichtmodule der Virtuellen Hochschule Bayern (VHB)

Das Angebot der Wahlpflichtmodule kann selbstständig um fachwissenschaftliche Wahlpflichtfächer der VHB (Virtuelle Hochschule Bayern) ergänzt werden. Dafür gilt folgendes:

- Studierende informieren sich selbstständig über das VHB Angebot unter www.vhb.org.
- Vor Belegung des Fachs muss sich der Studierende bis spätestens 3 Wochen nach Semesterbeginn beim Studiengangleiter erkundigen, ob das VHB-Fach als fachwissenschaftliches Wahlpflichtfach des Studiengangs grundsätzlich angerechnet werden kann.
- Nach erfolgreicher Absolvierung des VHB-Fachs ist ein Antrag auf Anrechnung zu stellen.
- VHB-Fächer erscheinen nicht im Prüfungsangebot der Fakultät. Eine Anmeldung über die Systeme der THI ist nicht möglich.
- Prüfungstermin und Prüfungsort werden vom VHB-Kursleiter bestimmt. Eine terminliche Überschneidungsfreiheit mit THI-Prüfungen wird nicht garantiert.
- Studierende entscheiden selbstständig, ob sie sich ein VHB-Fach als fachwissenschaftliches Wahlpflichtfach anrechnen lassen wollen.

2.8 Duales Studium

In Kooperation mit ausgewählten Praxispartnern kann der Studiengang Cybersicherheit auch im dualen Studienmodell („Studium mit vertiefter Praxis“) absolviert werden. Dual Studierende arbeiten während der vorlesungsfreien Zeit im Kooperationsunternehmen und können so ihr im Studium erworbenes theoretisches Wissen mit Berufspraxis ergänzen. Zusätzlich wird das Praxissemester sowie die Abschlussarbeit im Unternehmen absolviert. Eine optimale Verzahnung von Theorie und Praxis ist gewährleistet durch die Qualitätsstandards von „hochschule dual“, der Dachmarke des dualen Studiums in Bayern (https://www.hochschule-dual.de/).

Die Vorlesungszeiten im dualen Studienmodell entsprechen den normalen Studien- und Vorlesungszeiten an der THI. Das Curriculum des dualen Studiengangmodells unterscheidet sich gegenüber dem regulären Studiengangkonzept in folgenden Punkten:

- **Praxissemester im Kooperationsunternehmen:** Dual Studierende absolvieren das Praxissemester im Kooperationsunternehmen.
- **Dual-Module:** Regelmäßig angeboten werden gesonderte FW-Fächer für Dual-Studierende. Diese Veranstaltungen werden an der Hochschule bzw. einem Dualpartner durchgeführt. Angeboten werden auch gesonderte Projekte sowie separate Praxisseminare für Dualstudierende. Eine Anrechnung von Projekten und Praxisseminaren über außer-hochschulisch erworbene Kompetenzen aus dem Lernort Unternehmen ist möglich. Einzelne Veranstaltungen werden nach Möglichkeit von Lehrbeauftragten der Kooperationsunternehmen durchgeführt.
- **Abschlussarbeit im Kooperationsunternehmen:** Im dualen Studienmodell wird die Abschlussarbeit bei dem Kooperationsunternehmen geschrieben, i.d.R. über ein praxisrelevantes Thema mit Bezug zum Studienschwerpunkt. Die Erstbetreuung erfolgt durch einen Dozenten aus dem Studiengang Cybersicherheit.
- Organisatorisch zeichnet sich das duale Studiengangmodell durch folgende Bestandteile aus:
- **Einführungsveranstaltung:** Im Rahmen der Semesteröffnung und der Informationsveranstaltungen des Studiengangleiters zu Studienbeginn wird eine gesonderte Veranstaltung für Dualstudierende angeboten.
- **Mentoring:** Zentrale Ansprechpartner für Dualstudierende in der Fakultät sind die jeweiligen Studiengangleiter. Diese organisieren jährlich ein Mentoring-Treffen mit den Dualstudierenden des jeweiligen Studiengangs.
- **Qualitätsmanagement:** In den Evaluationen und Befragungen an der THI zur Qualitätssicherung der Studiengänge sind separate Frageblöcke für das duale Studium enthalten.
- **„Forum dual“:** Organisiert vom Career Service und Studienberatung (CSS) findet einmal jährlich das „Forum dual“ statt. Dieses fördert den fachlich-organisatorischen Austausch zwischen den dualen Kooperationspartnern und der Fakultät und dient zur Qualitätssicherung der dualen Studienprogramme. Zu dem Termin geladen sind alle Kooperationspartner im dualen Studium sowie Vertreter und Dualstudierende der Fakultät.

Weiterführende Informationen zum Dualen Studium und den aktuellen Unternehmenspartnern des Studiengangs User Experience Design Bachelor sind unter https://www.thi.de/studium/studienangebote/duales-studium zu finden.

Formalrechtliche Regelungen zum dualen Studium für alle Studiengänge der THI sind in der APO (s. §§ 17, 29 und 30) und der Immatrikulationssatzung (s. §§ 8b, 9 und 18) geregelt.

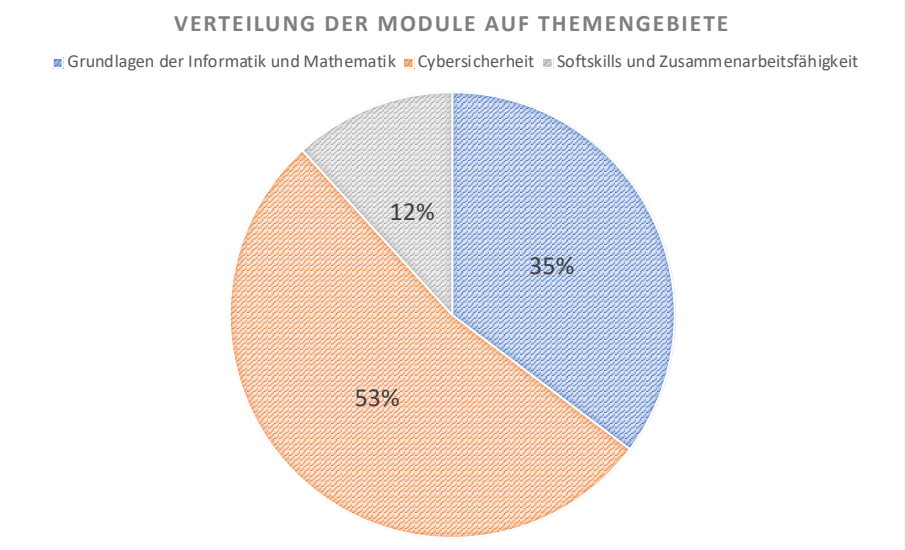
2.9 Konzeption

Die Entwicklung des Studiengangs Bachelor Cybersicherheit wurde durch die strategische Initiative der Hochschulpräsidiums der Technischen Hochschule Ingolstadt initiiert. Der Studiengang wurde im Rahmen des Arbeitskreises „Cybersicherheit“ an der Fakultät Informatik entwickelt. Der Arbeitskreis bestand aus Kollegen der Fakultät Informatik sowie folgenden Experten aus Wirtschaft, Lehre und Forschung:

- Prof. Dr.-Ing. Thomas Schreck (Professor für IT-Sicherheit und IT-Sicherheitsmanagement an der Hochschule München)
- Stefan Vollmer (Divisionsleiter Cyber- und Informationsraum bei der ESG Elektroniksystem- und Logistik GmbH)

3 Qualifikationsprofil

Im Fokus des Studiengangs steht der technische Schutz von Systemen und Anwendungen. Der Studiengang vermittelt ein breites Spektrum der technischen Aspekte der Cybersicherheit sowie Kenntnisse des rechtlichen Rahmens, der ethischen Leitlinien und betriebswirtschaftlicher Aspekte der Cybersicherheit. Somit wird das Wissen vermittelt, das notwendig ist, um später im Berufsleben vielfältige technische Aufgaben im Bereich Cybersicherheit wahrnehmen zu können. Des Weiteren wird durch das im Studium vermittelte Grundlagenwissen das Fundament für ein lebenslanges Lernen gelegt.



3.1 Leitbild

Der Studiengang integriert das Leitbild der Lehre auf folgende Weise:

Wir bereiten unsere Studierenden auf die Herausforderungen der Zukunft vor:

- Breites Verständnis von Problemstellungen der Cybersicherheit im Kontext der Digitalisierung.
- Grundlagenausbildung in der Informatik, um zur Anwendung von Methoden der Cybersicherheit schnell in verschiedene Anwendungsszenarien der Digitalisierung einsteigen zu können.
- Vermittlung zukunftsweisender Kompetenzen und Technologien, z.B. Künstliche Intelligenz.

Wir befähigen unsere Studierenden, Problemlösungen auf der Basis wissenschaftlicher Erkenntnisse zu erarbeiten:

- Vermittlung solider mathematischer Kenntnisse zur Einschätzung aktueller Entwicklungen im Bereich kryptographischen Verfahren.
- Vermittlung verschiedener Methoden zur Modellierung von Aspekten der Cybersicherheit.
- Theoriefächer im Bereich Cybersicherheit zur Stärkung der Fachkompetenz.
- Argumentationskompetenz zu den in der Cybersicherheit häufig auftretenden ethischen und rechtlichen Fragestellungen.

Wir eröffnen unseren Studierenden herausragende regionale und internationale Perspektiven:

- Einordnung der Studieninhalte in die nationale und internationale Cybersicherheitslandschaft.
- Die Englischkompetenz wird durch mindestens ein Modul mit Unterrichtssprache Englisch ab dem zweiten Semester gestärkt.
- Intensives Kennenlernen der Werkzeuge und Methoden, die in der Cybersicherheit eingesetzt werden als berufliche Basiskompetenz zu Beginn der Karriere.
- Vermittlung von nationalen und internationalen Standards der Cybersicherheit.

Wir lehren und lernen im persönlichen Austausch:

- Intensiver Austausch zwischen Lehrenden, Studierenden und Praxisexperten
- Projekt- und praxisbezogene Arbeiten
- Kennenlernen der Facetten des projekthaften Arbeitens: Arbeiten alleine vs. das Arbeiten in unterschiedlichen Gruppengrößen

Wir helfen allen Studierenden, ihr individuelles Potenzial zu entdecken und auszuschöpfen:

- Methodisches Entwickeln von Ideen und der eigenen Kreativität, insbesondere Ausbildung…
    - des für die Cybersicherheit besonders wichtigen „Out-of-the-box Thinking“

  - des für die Cybersicherheit besonders wichtigen Denkens im Systemkontext
- Start-up- und unternehmerische Kompetenz durch starke Umsetzungskompetenz

3.2 Studienziele

3.2.1 Fachspezifische Kompetenzen des Studiengangs

Die Studieninhalte wurden entsprechend den Anforderungen aus Industrie- und Mittelstand sowie des Qualifikationsrahmens für deutsche Hochschulabschlüsse definiert.

Für den Bachelorstudiengang müssen die allgemeinen Zulassungsvoraussetzungen für ein Studium an Hochschulen für angewandte Wissenschaften erfüllt sein.

Die vermittelten Fachspezifischen Kompetenzen verteilen sich auf die beiden Bereiche „Informatik/Mathematik“ und „Cybersicherheit“.

Absolventen des Studiengangs verfügen über die Fachkompetenzen, um

- sichere Systeme und Anwendungen zu planen und zu realisieren unter Verwendung von existierenden Security Komponenten und Konzepten.
- die IT-Sicherheit von Systemen und Anwendungen während Planung, Entwicklung und Betrieb zu überprüfen und zu beurteilen.
- ein vorgegebenes Schutzniveau im Betrieb von Systemen zu garantieren, Sicherheitsvorfälle zu untersuchen und erste Gegenmaßnahmen einzuleiten.
- Zertifizierungen vorzubereiten und durchzuführen.

3.2.2 Fachübergreifende Kompetenzen des Studiengangs

Folgende überfachlichen Kompetenzen sind von besonderer Bedeutung für den Studiengang.

Methodenkompetenzen:

Absolventen des Studiengangs…

- können Problemstellungen analysieren, übergreifende Zusammenhänge erkennen, Grundlagen und Prinzipien bei der Problemlösung umzusetzen, Lösungen technisch bewerten sowie Entscheidungsvorlagen aufzubereiten.
- sind fähig, wissenschaftlich zu arbeiten und wissenschaftliche Erkenntnisse in die berufliche Praxis zu transferieren.
- können interdisziplinär arbeiten und sich schnell in neue Anwendungsdomänen einarbeiten.

Sozialkompetenzen:

Absolventen des Studiengangs…

- können komplexe Aufgabenstellungen allein und im Team bearbeiten (Kommunikations- und Teamfähigkeit).
- können ihre Tätigkeit in den gesamtstaatlichen und gesamtgesellschaftlichen Kontext einordnen und handeln in diesem Kontext verantwortungsvoll.
- können einen wissenschaftlichen Diskurs führen.

Selbstkompetenzen:

Absolventen des Studiengangs…

- können überzeugend kommunizieren und argumentieren, insbesondere gegenüber dem höheren Management.
- haben grundlegende Kompetenzen im Bereich Projektmanagement und Teamarbeit.
- können sich selbst organisieren.
- können sich selbständig Wissen über neue Angriffs- und Schutzmethoden aneignen.
- können komplexe Aufgabenstellungen bearbeiten.
- können komplexe Zusammenhänge selbständig erschließen.
- können analytisch und lösungsorientiert denken.
- können zielorientiert und selbständig arbeiten.
- können Entscheidungen treffen.

3.2.3 Prüfungskonzept des Studiengangs

Bei der Entwicklung des Studiengangs wurde darauf geachtet, dass unterschiedlichste Prüfungsformen adäquat zum Einsatz kommen. Im Curriculum finden sich die Prüfungsformen schriftliche Prüfung, mündliche Prüfung, Seminararbeit, Projektarbeit und Leistungsnachweis (mit praktischen Aufgabenstellungen, schriftlichen Fallbearbeitungen oder Kurzreferaten).

Die folgende Tabelle gibt einen Überblick über den Einsatz der Prüfungsformen:

Lfd. Nr.	Modul	Art der Lehrveranstaltung	Prüfungsform
1	**Einführungsprojekt**	Pr	LN
2	**Grundlagen der Programmierung 1**		
2.1	Grundlagen der Programmierung 1	SU/Ü	schrP
2.2	Praktikum Grundlagen der Programmierung 1	Pr	LN
3	**Grundlagen der Programmierung 2**		
3.1	Grundlagen der Programmierung 2	SU/Ü	schrP
3.2	Praktikum Grundlagen der Programmierung 2	Pr	LN
4	**Einführung in die Informatik 1**	SU/Ü	schrP
5	**Einführung in die Informatik 2**		
5.1	Einführung in die Informatik 2	SU/Ü	schrP
5.2	Praktikum Einführung in die Informatik 2	Pr	LN
6	**Grundlagen der IT-Sicherheit**	SU/Ü	schrP
7	**Mathematik 1**		
7.1	Mathematik 1	SU	schrP
7.2	Übung zu Mathematik 1	Ü	
8	**Mathematik 2**		
8.1	Mathematik 2	SU	schrP
8.2	Übung zu Mathematik 2	Ü	
9	**Gesellschaftliche Verantwortung sowie Innere und Äußere Sicherheit**	SU/Ü	schrP
10	**Software-Entwicklungsmethodik**	SU/Ü	schrP
11	**Sichere Systeme**	SU/Ü	schrP

Lfd. Nr.	Modul	Art der Lehrveranstaltung	Prüfungsform
12	**Angewandte Mathematik für IT-Sicherheit**		
12.1	Angewandte Mathematik für IT-Sicherheit	SU	schrP
12.2	Übung zu Angewandte Mathematik für IT-Sicherheit	Ü	
13	**Netzwerke**		
13.1	Netzwerke	SU/Ü	schrP
13.2	Praktikum Netzwerke	Pr	LN
14	**Softwaresicherheit & Security Testing**	SU/Ü	schrP
15	**Software-Design, Software-Architektur und Datenbanken**		
15.1	Software-Design, Software-Architektur und Datenbanken	SU/Ü	schrP
15.2	Praktikum Software-Design, Software-Architektur und Datenbanken	Pr	
16	**Web-Technologien**	SU/Ü	schrP
17	**Ethical Hacking Praktikum**	Pr	LN
18	**Protokolle der Netzsicherheit**	SU/Ü	schrP
19	**Security Architektur & Security Engineering**		
19.1	Security Architektur & Security Engineering	SU/Ü	schrP
19.2	Praktikum zu Security Architektur & Security Engineering	Pr	LN
20	**Projekt-, Qualitäts- und Risikomanagement**	SU/Ü	schrP
21	**Recht für IT-Sicherheit und Datenschutz**	SU/Ü	schrP
22	**Fachwissenschaftliches Seminar**	S	SA
23	**Cloud-Architekturen und -Dienste**	SU/Ü	schrP
24	**Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit**		
24.1	Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit	SU/Ü	schrP

Lfd. Nr.	Modul	Art der Lehrveranstaltung	Prüfungsform
24.2	Praktikum Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit	Pr	LN
25	**Incidence Response und Netzwerkmonitoring**	SU/Ü	schrP
26	**Sichere Netzwerkarchitekturen und Sicherheit vernetzter Anwendungen**	SU/Ü	schrP
27	**Projekt**	Pr	Proj
28	**Grundlagen der Betriebswirtschaft und des Gründertums**	SU/Ü	schrP
29	**Fachwissenschaftliche Wahlpflichtmodule**	SU/Ü/Pr	schrP, mPr oder SA
30	**Bachelorarbeit**		
30.1	Seminar Bachelorarbeit	S	schrP, mPr oder SA
30.2	Bachelorarbeit		BA

Legende

schrP	schriftliche Prüfung	Die schriftliche Prüfung ist eine Klausur im Umfang von 90 Minuten, sofern nichts anderes bestimmt ist.
mdlP	mündliche Prüfung	Die mündliche Prüfung ist eine Befragung im Umfang von 15 Minuten, sofern nichts anderes bestimmt ist.
prP	praktische Prüfung	In der praktischen Prüfung ist am Beispiel einer Aufgabe der Nachweis zu führen, dass die notwendigen Fähigkeiten zur Lösung dieser Aufgabe beherrscht werden. Die Dauer beträgt 15 Minuten, sofern nichts anderes bestimmt ist.
LN	Leistungsnachweis	Bei dem Leistungsnachweis handelt es sich um eine Bearbeitung einer modulspezifisch festgelegten Anzahl von modulspezifischen praktischen Aufgabenstellungen, schriftlichen Fallbearbeitungen oder Kurzreferaten. Von diesen ist ein festgelegter Anteil erfolgreich zu bearbeiten, um den Leistungsnachweis zu bestehen. Das Nähere wird vom Fakultätsrat im Studienplan festgelegt. Bewertung durch das Prädikat „mit Erfolg abgelegt“ oder „ohne Erfolg abgelegt“. Der Leistungsnachweis muss bestanden sein.
StA	Studienarbeit	Die Studienarbeit ist eine Hausarbeit ohne mündliche Präsentation. Umfang der Hausarbeit laut APO THI: 3000 bis 6000 Wörter, ca. 10 bis 20 Seiten. Die Arbeit ist mit einem Texteditor zu erstellen.

SA	Seminararbeit	Die Seminararbeit ist eine Hausarbeit mit mündlicher Präsentation. Umfang der Hausarbeit laut APO THI: 3000 bis 6000 Wörter, ca. 10 bis 20 Seiten. Die Arbeit ist mit einem Texteditor zu erstellen. Die mündliche Präsentation hat einen Umfang von 30 bis 45 Minuten. Die mündliche Präsentation kann auch während des Semesters gehalten werden.
ProjA	Projektarbeit	Die Projektarbeit ist eine Gruppenarbeit, bei der eine gemeinsame Aufgabenstellung in der Gruppe zu erarbeiten ist. Jeder Teilnehmer muss einen eigenen Beitrag zur Lösung der gemeinsamen Aufgabe erbringen, einen Teil des Projektberichts erstellen und End- oder Zwischenergebnisse des Projekts mündlich präsentieren. Umfang des Projektberichts laut APO: 1500 bis 7500 Wörter, ca. 5 bis 25 Seiten. Umfang der mündlichen Präsentation laut APO: 15 bis 45 Minuten. Der Projektbericht ist mit einem Texteditor zu erstellen.
PrB	Praktikumsbericht	Der Praktikumsbericht soll über die während des Praktikums durchgeführten Tätigkeiten informieren. Der Umfang beträgt 8 bis 25 Seiten (ohne Deckblätter und Verzeichnisse). Näheres wird im Studienplan festgelegt. Der Bericht ist mit einem Texteditor zu erstellen.
BA	Bachelorarbeit	Schriftliche Abschlussarbeit im Bachelorstudiengang. Umfang 40 – 60 Seiten (ohne Deckblätter, Verzeichnisse und Anhänge). Die Arbeit ist mit einem Texteditor zu erstellen.

Die verbindlichen Regelungen zu Prüfungen finden sich in der Anlage zur Studien- und Prüfungsordnung für den Bachelorstudiengang Cybersicherheit in der Fassung vom 13.12.2021 ab WS 2022/23 und in der Allgemeinen Prüfungsordnung (APO) der Technischen Hochschule Ingolstadt.

3.2.4 Anwendungsbezug des Studiengangs

Alle Lehrenden haben einen langjährigen Hintergrund in der Industrie und/oder eine überdurchschnittliche akademische Qualifikation.

Die hohe Anwendungsrelevanz wird durch die konsequente Ausrichtung des Studiengangs an den Erfordernissen der Wirtschaft gewährleistet. Die Vertiefung erfolgt anhand von Übungen und Projektarbeiten, welche einen Bezug zu aktuellen und relevanten Themenstellungen haben.

Die Ausrichtung und der Praxisbezug wird mit Hilfe des Fachbeirats sicherstellt.

3.2.5 Beitrag einzelner Module zu den Studiengangzielen

In der nachfolgenden Tabelle ist die Zuordnung der einzelnen Module und deren Beitrag zu den Kompetenzfeldern „Fachkompetenz Informatik/Mathematik“, „Fachkompetenz Cybersicherheit“ und „Sozialkompetenz“, „Methoden-& und Selbstkompetenz“ aufgelistet.

Lfd. Nr.	Modul	Fachkompetenz Informatik/Mathematik	Fachkompetenz Cybersicherheit	Sozialkompetenz	Methoden- & Selbstkompetenz
1	Einführungsprojekt	+	+	++	+
2	Grundlagen der Programmierung 1	++	0	+	0
3	Grundlagen der Programmierung 2	++	0	+	+
4	Einführung in die Informatik 1	++	0	0	0
5	Einführung in die Informatik 2	++	0	+	+
6	Grundlagen der IT-Sicherheit	+	++	0	+
7	Mathematik 1	++	+	0	0
8	Mathematik 2	++	+	0	0
9	Gesellschaftliche Verantwortung sowie Innere und Äußere Sicherheit	0	+	0	++
10	Software-Entwicklungsmethodik	++	+	+	+
11	Sichere Systeme	+	++	0	0
12	Angewandte Mathematik für IT-Sicherheit	++	+	0	0
13	Netzwerke	++	+	+	0
14	Softwaresicherheit & Security Testing	+	++	0	+
15	Software-Design, Software-Architektur und Datenbanken	++	+	+	0

Lfd. Nr.	Modul	Fachkompetenz Informatik/Mathematik	Fachkompetenz Cybersicherheit	Sozialkompetenz	Methoden- & Selbstkompetenz
16	Web-Technologien	++	+	0	0
17	Ethical Hacking Praktikum	+	++	+	++
18	Protokolle der Netzsicherheit	+	++	0	0
19	Security Architektur & Security Engineering	+	++	+	0
20	Projekt-, Qualitäts- und Risikomanagement	0	+	++	++
21	Recht für IT-Sicherheit und Datenschutz	0	0	++	++
22	Fachwissenschaftliches Seminar	/	/	/	/
23	Cloud-Architekturen und -Dienste	++	+	0	0
24	Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit	++	++	+	0
25	Incidence Response und Netzwerkmonitoring	0	++	+	0
26	Sichere Netzwerkarchitekturen und Sicherheit vernetzter Anwendungen	0	++	0	0
27	Projekt	++	++	++	++
28	Grundlagen der Betriebswirtschaft und des Gründertums	0	0	++	++
29	Fachwissenschaftliche Wahlpflichtmodule	/	/	/	/
30	Bachelorarbeit	++	++	+	++

3.3 Mögliche Berufsfelder

Die Absolventen des Studiengangs sind v.a. für Fach- und Führungsaufgaben in folgenden Bereichen vorbereitet:

- Security Operations Center / Abteilung Cybersicherheit
- Information Risk Management (Prüfung von IT-Systemen und Beratung)
- Softwareentwicklung oder Systementwicklung
- IT-Abteilung

Bei den zukünftigen Tätigkeitsfeldern der Absolventen stehen folgende Branchen im Fokus:

- Mobilitätsanbieter
- Gesundheitssystem (Ärzte, Kliniken, Krankenkassen, eHealth etc.)
- Public Security
- Finanzbereich, eCommerce, FinTec
- Weitere Betreiber von kritischen Infrastrukturen (KRITIS)

Darüber hinaus haben Absolventen auch sehr gute Chancen als Selbständige oder als Angestellte in Unternehmen, welche für Ihre Produktion oder Dienstleistungserfüllung auf Informationstechnologie angewiesen sind.

4 Modulbeschreibungen

4.1 Allgemeine Pflichtmodule

Einführungsprojekt			
Modulkürzel:	CSI_EIN	**SPO-Nr.:**	1
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Eggendorfer, Tobias
Leistungspunkte / SWS:	2 ECTS / 2 SWS
Arbeitsaufwand:	Kontaktstunden: 23 h Selbststudium: 27 h Gesamtaufwand: 50 h
Lehrveranstaltungen des Moduls:	Einführungsprojekt
Lehrformen des Moduls:	Prj - Projekt
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:

Das Einführungsprojekt gilt als bestanden, wenn die Studentin / der Student an allen Tagen anwesend war, die fachwissenschaftlichen Aufgabenstellungen bearbeitet und präsentiert wurden, sowie die Einführung in die Bibliothek bearbeitet wurde.

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach der erfolgreichen Teilnahme an dem Modul

- können die Studierenden Anwendungsgebiete der Cybersicherheit benennen und ausgewählte Einsatzbeispiele erläutern.
- sind die Studierenden in der Lage, fachspezifische Informationen zielgerichtet auf fachwissenschaftlichem Niveau zu recherchieren, sowie
- eine einfache, fachspezifische Themenstellung in Zusammenarbeit mit anderen Studierenden geeignet aufzubereiten und zu präsentieren.

• sind die Studierenden mit grundlegenden Lernstrategien und Strategien des Zeitmanagements zur Organisation ihres Studiums vertraut und • sind in der Lage, sich selbst zu organisieren, in kleinen Teams erfolgreich zu arbeiten und Arbeitsaufträge selbständig durchzuführen.
Inhalt:
• Grundlagen fachwissenschaftlicher Recherche zu fachspezifischen Themen (Recherchetechniken und Informationsquellen) inkl. Bibliothekseinführung • Aufbereitung und Präsentation von spezifischen Themenstellungen zu Cybersecurity in Kleingruppen • Bearbeitung von fachspezifischen Aufgaben in Kleingruppen & Teambuilding (z.B. Entwicklung von einfachen Programmen in Python, Verwendung von Security-Tools, Kreativaufgaben) • Gemeinsame Projektarbeit • Lernstrategien und Zeitmanagement im Studium
Literatur:
Wird zu Beginn bekannt gegeben
Anmerkungen:
Für Dual-Studierende wird eine eigene Gruppe gebildet. Im Rahmen einer Einführungsveranstaltung findet eine eigene Kick-Off Veranstaltung statt.

Grundlagen der Programmierung 1

Modulkürzel:	FFI_GP1	**SPO-Nr.:**	2
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Regensburger, Franz
Leistungspunkte / SWS:	7 ECTS / 6 SWS
Arbeitsaufwand:	Kontaktstunden: 70 h Selbststudium: 105 h Gesamtaufwand: 175 h
Lehrveranstaltungen des Moduls:	2.1: Grundlagen der Programmierung 1 2.2: Praktikum Grundlagen der Programmierung 1
Lehrformen des Moduls:	2.1: SU/Ü - seminaristischer Unterricht/Übung 2.2: Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

2.1: schrP90 - schriftliche Prüfung, 90 Minuten

2.2: LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:

Im Rahmen des Praktikums müssen mehrere Testate (Programmieraufgaben in C) erworben werden. Bei erfolgreicher Bearbeitung der Aufgabenstellung wird vom Dozenten jeweils ein Testat vergeben.

Die Lösungen dürfen und sollen zur Förderung der sozialen und fachlichen Kompetenz in Kleingruppen erarbeitet werden.

Insgesamt müssen vier Aufgaben bearbeitet werden, die wesentliche Themen der Vorlesung behandeln. Die fertigen Lösungen sind einzeln innerhalb eines festen Terminrasters (alle 14 Tage ein Testat) individuell von den Teilnehmern zu präsentieren, wobei auch Fragen zum Lösungskonzept und zum erstellten Programm zu beantworten sind.

Nur wenn alle vier Testate rechtzeitig erworben werden, gilt der Leistungsnachweis als erbracht.

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung,

- kennen die Studierenden allgemeine Begriffe der Informatik.
- kennen die Studierenden in Grundzügen die historische Entwicklung von Programmiersprachen.

- können die Studierenden einfache Probleme logisch erfassen und selbständig eine algorithmische Lösung dafür erstellen.
- können die Studierenden in einer höheren imperativen Programmiersprache vorgegebene oder selbst entwickelte Algorithmen implementieren, insbesondere in C.
- sind die Studierenden in der Lage, Dienste des Betriebssystems und eine Entwicklungsumgebung zu nutzen.
- sind die Studierenden in der Lage, gemeinsam in kleinen Teams (soziale Kompetenz) Programmieraufgaben zu bearbeiten.

Nach dem Besuch des Praktikums

- sind die Studierenden in der Lage, vorgegebene Code-Teile zu verstehen und selbständig Erweiterungen im Code vorzunehmen.
- können die Studierenden auch umfangreichere C-Programme (zwischen 500 - 2000 Zeilen Code) erstellen.
- können die Studierenden die wesentlichen Komponenten einer Entwicklungsumgebung (Editor, Compiler Debugger und Build-Tool) bedienen.
- können die Studierenden gemeinsam in kleinen Teams (soziale Kompetenz) Programmieraufgaben lösen.

Inhalt:

- Grundbegriffe der Informatik, Phasen und Werkzeuge der Software-Entwicklung, Struktogramme, Grundbegriffe und Prinzipien der imperativen Programmierung
- Programmiersprachen (allgemein und speziell Sprache C)
- Ablaufsteuerung, primitive Datentypen in C
- Getrennte Übersetzung und Entwicklungsumgebung (Editor, Build-Tool, Debugger)
- Enumerationen und Datentyp bool
- Funktionen, Unterprogrammtechnik, Parameterübergabe, Auf- und Abbau des Stacks
- Records
- Arrays
- Pointer
- Statische und dynamische Speicherobjekte, Gültigkeit, Sichtbarkeit und Lebensdauer
- Verkettete Listen und andere Speichergeflechte
- String-Funktionen der Standardbibliothek

Im Praktikum wird ein interaktives Spiel (Worm) mit einfacher Symbolgrafik auf Basis der Curses-Bibliothek erstellt.

Die Programmierung in der Sprache C erfolgt auf Basis einer virtuellen Linux-Maschine, deren Image in allen Rechner-Pools der Fakultät vorinstalliert ist.

Dieses Image kann weiterhin von allen Studierenden kopiert werden und auf dem eigenen PC genutzt werden.

In der virtuellen Maschine wird ausschließlich OpenSource-Software verwendet, so dass das Image der virtuellen Maschine beliebig oft kopiert und weitergegeben werden darf.

Das Image enthält auch Software für die höheren Semester, so dass die virtuelle Linux-Maschine während des gesamten Studiums genutzt werden kann.

Literatur:

- GOLL, Joachim, BRÖCKL, Ulrich, DAUSMANN, Manfred, 2003. *C als erste Programmiersprache: Vom Einsteiger zum Profi* [online]. Wiesbaden: Vieweg+Teubner PDF e-Book. ISBN 978-3-322-92700-2, 978-3-322-92701-9. Verfügbar unter: http://dx.doi.org/10.1007/978-3-322-92700-2.
- ERNST, Hartmut, SCHMIDT, Jochen, BENEKEN, Gerd Hinrich, 2016. *Grundkurs Informatik: Grundlagen und Konzepte für die erfolgreiche IT-Praxis - Eine umfassende, praxisorientierte Einführung* [online]. Wiesbaden: Springer Fachmedien Wiesbaden PDF e-Book. ISBN 978-3-658-14634-4, 978-3-658-14633-7. Verfügbar unter: http://dx.doi.org/10.1007/978-3-658-14634-4.

Anmerkungen:
Hierfür wird den Studierenden ein gebrauchsfertiges Image einer virtuellen Maschine für das Selbststudium zuhause zur Verfügung gestellt, welches unter allen Plattformen mittels VirtualBox oder anderer gängiger Hypervisor zur Ausführung gebracht werden kann. Des Weiteren wird dieses Image in den PC-Pools der Fakultät zur Verfügung gestellt.

Grundlagen der Programmierung 2

Modulkürzel:	FFI_GP2	**SPO-Nr.:**	3
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Gold, Robert	
Leistungspunkte / SWS:	7 ECTS / 6 SWS	
Arbeitsaufwand:	Kontaktstunden:	70 h
	Selbststudium:	105 h
	Gesamtaufwand:	175 h
Lehrveranstaltungen des Moduls:	3.1: Grundlagen der Programmierung 2 3.2: Praktikum Grundlagen der Programmierung 2	
Lehrformen des Moduls:	3.1: SU/Ü - seminaristischer Unterricht/Übung 3.2: Pr - Praktikum	
Verwendbarkeit für andere Studiengänge:	Keine	

Prüfungsleistungen:

3.1: schrP90 - schriftliche Prüfung, 90 Minuten

3.2: LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:

Zum Bestehen des Praktikums müssen 5 Teilaufgaben von den Studierenden eigenständig und erfolgreich bearbeitet werden. Die 5 Teilaufgaben bauen aufeinander auf und ergeben am Ende ein Anwendungsprogramm mit graphischer Benutzeroberfläche. Als erfolgreich bearbeitet gilt eine Teilaufgabe, wenn sie erstens die den Studierenden zur Verfügung gestellten Unit-Tests besteht, zweitens eine Plagiatsprüfung ohne Beanstandung durchläuft und drittens eine ausreichende Quellcodequalität aufweist, die durch den Praktikumsbetreuer überprüft wird.

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung,

- sind die Teilnehmer in der Lage, grundlegende und weiterführende Konzepte der Objektorientierung zu verstehen und zu bewerten (Klassen und Objekte, Vererbung, abstrakte Klassen, Polymorphie, Lambda-Ausdrücke, generische Datentypen und Templates, Exceptions, grafische Benutzungsoberflächen, Threads).
- sind die Teilnehmer in der Lage, grundlegende technische Konzepte der Ausführung von C++-Programmen zu verstehen, mit anderen Programmiersprachen zu vergleichen und zu bewerten.

- sind die Teilnehmer in der Lage, einfache Klassendiagramme zu verstehen und zu erstellen.
- sind die Teilnehmer in der Lage, informationstechnische Aufgabenstellungen zu erfassen, Datenstrukturen und Benutzungsoberflächen dafür zu entwerfen und objektorientierte Software in C++ zu erstellen.
- nach der erfolgreichen Teilnahme am Praktikum sind die Studierenden in der Lage, informationstechnische Aufgabenstellungen zu erfassen, Datenstrukturen und Benutzungsoberflächen dafür zu entwerfen und objektorientierte Software in C++ unter Verwendung von Software-Werkzeugen (Editor, Debugger, Build-Tool etc.) zu erstellen.

Inhalt:

- Prinzipien der Objektorientierung
  - Klassen und Objekte
  - Vererbung und abstrakte Klassen
  - Polymorphie
  - Klassendiagramme
- Die Programmiersprache C++
  - Vor- und Nachteile
- Lambda-Ausdrücke
- Generische Datentypen und Templates
- Exceptions
- Ein-/Ausgabe
- Grafische Benutzungsoberflächen
- Threads
- Im Praktikum wird ein Anwendungsprogramm mit graphischer Benutzeroberfläche erstellt. Die Erstellung des Programms teilt sich in 5 Schritte auf, die begleitend zur Vorlesung, die Grundlagen der objektorientierten Programmierung in C++ behandeln. Folgende Themen werden dabei besonders vertieft:
  - einfache Klassen
  - Vererbung und Polymorphie
  - generische Datentypen und Templates
  - GUI Programmierung

Literatur:

- WILL, Torsten T., 2020. *C++: das umfassende Handbuch*. 2. Auflage. Bonn: Rheinwerk Verlag. ISBN 978-3-8362-7595-8
- BREYMANN, Ulrich, 2020. *C++ programmieren: C++ lernen – professionell anwenden – Lösungen nutzen* [online]. München: Carl Hanser Verlag PDF e-Book. ISBN 978-3-446-46551-0, 978-3-446-46470-4. Verfügbar unter: https://doi.org/10.3139/9783446465510.

Anmerkungen:

Keine Anmerkungen

Einführung in die Informatik 1

Modulkürzel:	FFI_INF1	**SPO-Nr.:**	4
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Margull, Ulrich
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Einführung in die Informatik 1
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach Besuch des Moduls

- haben die Studierenden ein Grundverständnis davon, wie Algorithmen (Folgen von maschinell ausführbaren Rechenschritten) auf Rechnern (programmgesteuerten Informationsverarbeitungssystemen) ausgeführt werden.
- können die Studierenden den Begriff des Algorithmus erläutern.
- sind die Studierenden in der Lage zu beurteilen, ob ein Problem berechenbar ist, d.h. ein Algorithmus zu seiner Lösung formuliert werden kann.
- sind die Studierenden in der Lage, die Komplexität eines gegebenen Algorithmus abzuschätzen.
- verstehen die Studierenden, wie ein Algorithmus auf einem Rechner ausgeführt werden kann.
- sind die Studierenden in der Lage den Aufbau eines Universalrechners und seine Arbeitsweise zu beschreiben.
- verstehen die Studierenden verschiedene fortgeschrittene Konzepte der Rechnerarchitektur, wie Cache, Pipelining.

Inhalt:

Algorithmen

- Algorithmenbegriff, Eigenschaften, Darstellungsformen
- Turing-Berechenbarkeit sowie LOOP-, WHILE-, GOTO-Berechenbarkeit
- Church-Turing-These
- Entscheidbarkeit, Halteproblem
- Komplexität und O-Notation
- Komplexitätsklassen, z.B. P und NP

Rechnerarchitektur

- Binäre Informationsdarstellung: natürliche, negative, gebrochene Zahlendarstellungen
- Digitale Schaltungen, Verknüpfungsglieder, Schaltnetze
- Speicherglieder, Register, Zähler, Schaltwerke
- Von Neumann-Rechner, Maschinenbefehle und -programme
- Fortgeschrittene Konzepte in heutigen Rechnerarchitekturen, wie Caching, Befehlspipelining, Mehrkern-Architekturen

Literatur:

- ERNST, Hartmut, SCHMIDT, Jochen, BENEKEN, Gerd Hinrich, 2020. *Grundkurs Informatik: Grundlagen und Konzepte für die erfolgreiche IT-Praxis – Eine umfassende, praxisorientierte Einführung* [online]. Wiesbaden: Springer Vieweg PDF e-Book. ISBN 978-3-658-30331-0. Verfügbar unter: https://doi.org/10.1007/978-3-658-30331-0.
- SCHÖNING, Uwe, 2009. *Theoretische Informatik - kurz gefasst*. Nachdruck der 5. Auflage. Heidelberg: Spektrum, Akad. Verl.. ISBN 978-3-8274-1824-1, 3-8274-1824-0
- ZIEGENBALG, J, O ZIEGENBALG und B ZIEGENBALG, 2010. *Algorithmen von Hammurapi bis Gödel*. 3. Auflage. ISBN 9783817118649
- BÖTTCHER, Axel, 2006. *Rechneraufbau und Rechnerarchitektur: mit 19 Tabellen* [online]. Berlin [u.a.]: Springer PDF e-Book. ISBN 3-540-20979-4, 978-3-540-20979-9. Verfügbar unter: https://doi.org/10.1007/3-540-44731-8.
- SIPSER, Michael, 2013. *Introduction to the theory of computation*. 3. Auflage. Boston, Mass.: Cengage Learning. ISBN 978-1-133-18781-3, 978-1-133-18779-0
- HELLMANN, Roland, 2022. *Rechnerarchitektur: Einführung in den Aufbau moderner Computer* [online]. München ; Wien: De Gruyter Oldenbourg PDF e-Book. ISBN 978-3-11-074179-7, 978-3-11-074191-9. Verfügbar unter: https://doi.org/10.1515/9783110741797.

Anmerkungen:

Bonuspunkteregelung: Für diese Vorlesung werden Bonuspunkte gemäß APO §25 Absatz (2) vergeben. Die Bonuspunkte betragen maximal 5% der in der Klausur vergebenen Punkte. Die genauen Bedingungen sind im Moodle-Kursraum zur Veranstaltung hinterlegt (Link: https://moodle.thi.de/moodle/mod/resource/view.php?id=312276).

Einführung in die Informatik 2

Modulkürzel:	FFI_INF2	SPO-Nr.:	5
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Margull, Ulrich
Leistungspunkte / SWS:	7 ECTS / 6 SWS
Arbeitsaufwand:	Kontaktstunden: 70 h Selbststudium: 105 h Gesamtaufwand: 175 h
Lehrveranstaltungen des Moduls:	5.1: Einführung in die Informatik 2 5.2: Praktikum Einführung in die Informatik 2
Lehrformen des Moduls:	5.1: SU/Ü - seminaristischer Unterricht/Übung 5.2: Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Die Anrechnung in anderen Studiengängen kann der Anrechnungstabelle der Fakultät entnommen werden.

Prüfungsleistungen:

5.1: schrP90 - schriftliche Prüfung, 90 Minuten

5.2: LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:

Voraussetzung für die Teilnahme an der schriftlichen Prüfung ist ein erfolgreich abgeschlossenes Praktikum.

Das begleitende Praktikum umfasst 8 Aufgaben, die vorbereitet und im Labor bzw. auf dem Rechner vorgeführt werden müssen. Für das Bestehen ist der erfolgreiche Abschluss von 7 der 8 Aufgaben notwendig.

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Programmierkenntnisse in C sowie Grundlagen der Rechnerarchitektur und Digitaltechnik

Angestrebte Lernergebnisse:

Nach Besuch von Teil 1 (Mikrocomputertechnik) des Moduls sind die Studierenden in der Lage,

- den Aufbau und die Entwicklung von Mikrocomputersystemen zu erläutern.
- typische Mikrocontroller und deren Speicherarten, wie SRAM und Flash zu erläutern und deren Einsatzzwecke zu bewerten.
- die wichtigsten Peripherals, wie GPIO, Timer, zu erklären und mittels Software anzusteuern.
- typische Problemstellungen der Mikrocomputertechnik zu analysieren und Implementierungen auf einem Mikrocontroller zu entwickeln und zu testen.

Nach Besuch von Teil 2 (Betriebssysteme) des Moduls sind die Studierenden in der Lage,

- die Aufgaben und Funktionen von Betriebssystemen zu erläutern.

- grundlegende Betriebssystemkonzepte zu verstehen sowie deren Implementierungen und mögliche Probleme beurteilen.
- einfache parallele Anwendungen für Betriebssysteme zu entwickeln und zu testen.
- bestehende Betriebssysteme einzuordnen und zukünftige Entwicklungen einzuschätzen.

Inhalt:

Teil 1 (Mikrocomputer)

- Architektur von Mikrocomputersystemen
- Aufbau von Mikroprozessoren und Mikrocontrollern
- Architektur von Steuergeräteprogrammen (Hauptschleife, Unterbrechungsmodus)
- Programmierung von Mikrocontrollern, hardwarenahes C, effiziente Programmstrukturen, Besonderheiten im Maschinenbefehlssatz und in der Befehlsabarbeitung von Mikrocontrollern
- Peripheriemodule von Mikrocontrollern (Ports, Timer, serielle Kommunikationsmodule, Analog-Digital Wandler)
- Speichertechniken und -bausteine (SRAM, DRAM, EEPROM, Flash)
- Busse und Systemstrukturen, Anbindung von Speicherbausteinen an Mikrocontroller

Teil 2 (Betriebssysteme)

- Aufgaben und Struktur von Betriebssystemen
- Parallelität: Prozesse und Threads, Scheduling, Interprozesskommunikation sowie Synchronisation
- Speicherverwaltung, virtueller Speicher
- Ein-/Ausgabe, Gerätetreiber
- Dateisysteme
- Virtualisierung

Literatur:

- BRINKSCHULTE, Uwe, UNGERER, Theo, 2010. *Mikrocontroller und Mikroprozessoren* [online]. Heidelberg [u.a.]: Springer PDF e-Book. ISBN 978-3-642-05397-9, 978-3-642-05398-6. Verfügbar unter: https://doi.org/10.1007/978-3-642-05398-6.
- GLATZ, Eduard, 2019. *Betriebssysteme: Grundlagen, Konzepte, Systemprogrammierung*. 4. Auflage. Heidelberg: dpunkt.verlag. ISBN 978-3-96088-839-0, 978-3-96088-840-6

Anmerkungen:

Bonuspunkteregelung: Für diese Vorlesung werden Bonuspunkte gemäß APO §25 Absatz (2) vergeben. Die Bonuspunkte betragen maximal 5% der in der Klausur vergebenen Punkte. Die genauen Bedingungen sind im Moodle-Kursraum zur Veranstaltung hinterlegt (Link: https://moodle.thi.de/mod/resource/view.php?id=342625).

Grundlagen der IT-Sicherheit

Modulkürzel:	CSI_GIS	**SPO-Nr.:**	6
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Eggendorfer, Tobias
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Grundlagen der IT-Sicherheit
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach der erfolgreichen Teilnahme an dieses Modul

- können die Studierenden die Teilbereiche der IT-Sicherheit benennen und Themen diesen Teilbereichen zuordnen.
- kennen die Studierenden grundlegende Begriffe der IT-Sicherheit und können diese sicher verwenden.
- kennen die Studierenden grundlegende Regularien der IT-Sicherheit.
- kennen die Studierenden die aktuellen Bedrohungen für IT-Systeme und Anwendungen.
- können Studierende Sicherheitsziele zum Schutz von IT-Systemen und Anwendungen formulieren.
- kennen die Studierenden grundlegende kryptographische Verfahren aus Sicht des Programmierers/Anwenders (Verschlüsselung, Digitale Signatur, Hash-Werte).
- kennen die Studierenden die Problematik der sicheren Schlüsseverteilung und können verschiedene Lösungsstrategien in konkreten Anwendungsfällen einsetzen.
- kennen die Studierenden die Problematik der sicheren Identität und können verschiedene Lösungsstrategien in konkreten Anwendungsfällen einsetzen.

- können Studierende einfache Programme in Python schreiben, um Problemstellungen der IT-Sicherheit zu lösen.
- können Studierende Werkzeuge der IT-Sicherheit einsetzen, um einfache Anwendungsprobleme zu lösen (z.B. Verschlüsselung von Daten).

Inhalt:

- Überblick über die Teilgebiete der IT-Sicherheit
- Bedrohungen für IT-Sicherheit
- Sicherheitsziele
- Kryptographische Bausteine aus Sicht des Programmierers/Anwenders (Verschlüsselung, Signatur, Hash-Funktion)
- Schlüsselverteilung, Zertifikate und PKI
- IT-Werkzeuge für Cybersicherheit
- Relevante Standards (z.B. ISO 27001 / BSI Grundschutz)
- Einführung in die Programmierung in Python

Literatur:

- ECKERT, Claudia, 2018. *IT-Sicherheit: Konzepte - Verfahren - Protokolle* [online]. München: De Gruyter Oldenbourg PDF e-Book. ISBN 978-3-11-056390-0. Verfügbar unter: https://doi.org/10.1515/9783110563900.
- BYRNE, Dennis , . *Full Stack Python Security*. ISBN 1617298824
- POHLMANN, Norbert, 2022. *Cyber-Sicherheit: das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung* [online]. Wiesbaden: Springer Vieweg PDF e-Book. ISBN 978-3-658-36243-0. Verfügbar unter: https://doi.org/10.1007/978-3-658-36243-0.

Anmerkungen:

Keine Anmerkungen

Mathematik 1

Modulkürzel:	FFI_MG1	**SPO-Nr.:**	7
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Lorencka, Joanna
Leistungspunkte / SWS:	6 ECTS / 5 SWS
Arbeitsaufwand:	Kontaktstunden: 58 h Selbststudium: 92 h Gesamtaufwand: 150 h
Lehrveranstaltungen des Moduls:	7.1: Mathematik 1 7.2: Übung zu Mathematik 1
Lehrformen des Moduls:	7.1: SU - seminaristischer Unterricht 7.2: Ü - Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

7.1: schrP90 - schriftliche Prüfung, 90 Minuten

7.2: O – ohne Leistungsnachweis

Weitere Erläuterungen:

Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Es werden die mathematischen Kenntnisse aus der Bayerischen Fachhochschulreife vorausgesetzt.

Angestrebte Lernergebnisse:

Nach Besuch des Moduls sind die Studierenden in der Lage,

- mathematische Denk- und Arbeitsweisen darzustellen, sowohl inhaltlich als auch vom unverzichtbaren Formalismus her.
- grundlegende mathematische Begriffe und Verfahren, die der Informatiker benötigt, wiederzugeben und zu übertragen und auf die in höheren Semestern aufgebaut werden kann.
- Beweisstrukturen zu verstehen und informatikrelevante Beweise durchzuführen.
- Grundlagen der Algebra, Logik und Wahrscheinlichkeitsrechnung wiederzugeben und auf fachspezifische Aufgaben anzuwenden.
- Grenzwertprozesse analysieren.
- Komplexe Zahlen in unterschiedliche Formen darzustellen, um Gleichungen und Ungleichungen zu lösen.

- Mit Matrizen zu rechnen, beispielsweise um lineare Gleichungssysteme zu lösen.
- Formel und Sätze aus der Differential- und Integralrechnung wiederzugeben, anzuwenden und zu interpretieren.

Inhalt:

- Abbildungen, Logische Schaltungen, Aussagenlogik, elementare Mengenlehre, Binärwörter, Binomialkoeffizienten, Boolesche Algebra, Quantorenlogik
- Einführung in die Wahrscheinlichkeitsrechnung
- Folgen und Reihen
- Komplexe Zahlen
- Matrizenkalkül
- Lineare Gleichungssysteme
- Differential- und Integralrechnung

Literatur:

- ERVEN, Joachim, 2011. *Taschenbuch der Ingenieurmathematik: Grundlagen - Formelsammlung - Tabellen*. München: De Gruyter. ISBN 978-3-486-71087-8, 3-486-71087-7
- TESCHL, G. und S. TESCHL, 2008. *Mathematik für Informatiker, Bd. 1*.
- HARTMANN, Peter, 2015. *Mathematik für Informatiker: ein praxisbezogenes Lehrbuch* [online]. Wiesbaden: Springer Vieweg PDF e-Book. ISBN 978-3-658-03415-3, 978-3-658-03416-0. Verfügbar unter: https://doi.org/10.1007/978-3-658-03416-0.
- KEMNITZ, Arnfried, 2019. *Mathematik zum Studienbeginn: Grundlagenwissen für alle technischen, mathematisch-naturwissenschaftlichen und wirtschaftswissenschaftlichen Studiengänge*. 12. Auflage. Wiesbaden: Springer Spektrum. ISBN 978-3-658-26604-2, https://doi.org/10.1007/978-3-658-26604-2

Anmerkungen:

Keine Anmerkungen

Mathematik 2

Modulkürzel:	FFI_MG2	**SPO-Nr.:**	8
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Lorencka, Joanna
Leistungspunkte / SWS:	6 ECTS / 5 SWS
Arbeitsaufwand:	Kontaktstunden: 58 h Selbststudium: 92 h Gesamtaufwand: 150 h
Lehrveranstaltungen des Moduls:	8.1: Mathematik 2 8.2: Übung zu Mathematik 2
Lehrformen des Moduls:	8.1: SU - seminaristischer Unterricht 8.2: Ü - Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

8.1: schrP90 - schriftliche Prüfung, 90 Minuten

8.2: O – ohne Leistungsnachweis

Weitere Erläuterungen:

Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach Besuch des Moduls sind die Studierenden in der Lage,

- analytische Funktionen in Potenzreihen zu entwickeln, speziell als Taylorpolynom, und den Fehler, der durch die Polynomdarstellung entsteht, mit Hilfe des Lagrangeschen Restglieds abzuschätzen.
- die Definition des Riemann Integrals den HDI und den Mittelwertsatz der Integralrechnung sowie die üblichen Integrationstechniken wie Substitution, partielle Integration, Integration über Partialbruchzerlegung und Potenzreihenentwicklung wiederzugeben.
- durch die vermittelte mathematische Basis, in Verbindung mit dem Modul "Mathematische Grundlagen 1", Aufgaben aus der Ingenieurmathematik zu lösen.
- die Grundlagen der linearen Algebra wie zum Beispiel die wichtigsten algebraischen Strukturen und die Eigenschaften linearer Abbildungen zu beschreiben.
- Eigenwerte und Eigenvektoren zu berechnen und Matrizen zu diagonalisieren.

- aus den Bereichen Kombinatorik und Modulararithmetik Grundkenntnisse abzurufen.
- grundlegende Konzepte aus der numerischen Mathematik bzw. Informatik wiederzugeben und diese anzuwenden.

Inhalt:

1. Analysis:
- Anwendungen der Differenzialrechnung
- Potenzreihen
- MacLaurin / Taylor- Reihen und deren Fehlerabschätzung
- Riemann Integral: Mittelwertsatz und HDI
- Integrationstechniken
- uneigentliche Integrale
- numerische Integration
- Bogenlänge, Mantelfläche und Volumen von Rotationskörpern

2. Algebra:
- Algebraische Strukturen: Gruppe, Ring, Körper, Vektorraum
- Lineare Abbildungen zwischen Vektorräumen
- Eigenwerte und Eigenvektoren
- Diagonalisierbarkeit von Matrizen und Hauptachsentransformation
- Modulare Arithmetik
- Kombinatorik

Literatur:

- TESCHL, Gerald und Susanne TESCHL, 2007. *Mathematik für Informatiker Band1: Diskrete Mathematik und Lineare Algebra*. 2. Auflage. Berlin Heidelberg: Springer. ISBN 978-3540708247
- TESCHL, Gerald und Susanne TESCHL, 2007. *Mathematik für Informatiker Band2: Analysis und Statistik*. 2. Auflage. Berlin Heidelberg: Springer. ISBN 978-3540724513
- HARTMANN, Peter, 2015. *Mathematik für Informatiker: ein praxisbezogenes Lehrbuch* [online]. Wiesbaden: Springer Vieweg PDF e-Book. ISBN 978-3-658-03415-3, 978-3-658-03416-0. Verfügbar unter: https://doi.org/10.1007/978-3-658-03416-0.

Anmerkungen:

Keine Anmerkungen

Gesellschaftliche Verantwortung sowie Innere und Äußere Sicherheit			
Modulkürzel:	CSI_GIA	**SPO-Nr.:**	9
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Uhl, Matthias
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Gesellschaftliche Verantwortung sowie Innere und Äußere Sicherheit
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

In der Veranstaltung werden die gesellschaftlichen Implikationen sowie die ethischen Grundlagen innerer und äußerer Sicherheit erarbeitet. Die Studierenden kennen nach Besuch der Veranstaltung die wesentlichen normativen Theorien zur Beurteilung innerer und äußerer Sicherheit und können diese kritisch reflektieren. Die Studierenden sind zudem in der Lage konkrete Fragestellungen aus dem Bereich der inneren und äußeren Sicherheit vor dem Hintergrund normativer Theorien abzuwägen und zu beurteilen. Es wird außerdem eine kritische Auseinandersetzung mit der eigenen ideologischen Position angeregt.

Inhalt:

- Was ist Ethik?
- Normative Theorien
- Normenbegründung unter Dissens
- Naturalistischer und moralistischer Fehlschluss
- Risikoethik
- Zum Begriff der Sicherheit

- Die Bedeutung von Empirie für die Sicherheitsforschung
- Zum Spannungsverhältnis von Freiheit und Sicherheit
- Pazifismus
- Cybersicherheit und der Zusammenhang von innerer und äußerer Sicherheit

Literatur:

- LIAO, S. Matthew, 2020. *Ethics of artificial intelligence*. New York, NY: Oxford University Press. ISBN 978-0-19-090503-3, 978-0-19-090504-0
- BIRNBACHER, Dieter, 2013. *Analytische Einführung in die Ethik*. 3. Auflage. ISBN 978-3110313611

Anmerkungen:

Keine Anmerkungen

Software-Entwicklungsmethodik

Modulkürzel:	FFI_SWM	**SPO-Nr.:**	10
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hagerer, Andreas
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Software-Entwicklungsmethodik
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach Besuch des Moduls

- kennen die Studierenden die grundlegenden Schritte des System-Engineerings.
- kennen die Studierenden existierende Qualitätsmodelle und deren Bedeutung für die Entwicklung von Software.
- kennen die Studierenden aktuelle Reifegradmodelle für Prozesse und deren Bedeutung.
- kennen die Studierenden die grundlegenden Strategien des Testens.
- kennen die Studierenden typische Modelle für das Vorgehen in einem Software-Entwicklungsprojekt.
- können die Studierenden Anforderungen an ein Softwaresystem strukturiert beschreiben.
- können die Studierenden ausgewählte Diagramme der UML zur Beschreibung und Dokumentation einer Software einsetzen.
- können die Studierenden Methoden und die Instrumente des Software-Engineerings für die Analyse und Tests situationsgerecht einsetzen.

Selbst- und Sozialkompetenzen:
Nach Abschluss des Moduls

- können Studierende Anforderungsdokumentationen lesen, interpretieren und diskutieren.
- verfügen Studierende über ein ausreichendes Abstraktionsvermögen und analytisches Denken, um komplexe Problemstellungen in Modellen zu beschreiben.
- können Studierende auf einem angemessenen Abstraktionsniveau innerhalb eines interdisziplinären Projektteams Ergebnisse aus der Analysephase einer Software-Entwicklung kommunizieren und Lösungen argumentieren.

Inhalt:

- Grundlagen zu Software Engineering
- Software Qualität (ISO 25010)
- Requirements Engineering einschließlich relevanter UML-Diagramme (Vorgehensweise und Bedeutung, Stakeholder, Systemkontext, Erhebungsmethoden, Dokumentation)
- Implementieren von Software (Dokumentation, Konventionen)
- Testen von Software (statische Tests, dynamische Tests, Whitebox- und Blackboxtesting)
- Vorgehensmodelle (z.B. Wasserfall, V-Modell und Scrum)
- Prozesse / Prozessreife-Modelle wie CMMI oder SPICE

Literatur:

- SOMMERVILLE, Ian, 2020. *Engineering software products: an introduction to modern software engineering*. F. Auflage. Hoboken, NJ: Pearson. ISBN 978-0-13-521064-2
- RUPP, Chris, QUEINS, Stefan, 2012. *UML 2 glasklar: Praxiswissen für die UML-Modellierung* [online]. München: Hanser PDF e-Book. ISBN 978-3-446-43197-3. Verfügbar unter: https://doi.org/10.3139/9783446431973.
- BALZERT, Helmut, 2011. *Lehrbuch der Software-Technik / [3]. Entwurf, Implementierung, Installation und Betrieb*. 3. Auflage. Heidelberg [u.a.]: Spektrum, Akad. Verl.. ISBN 978-3-8274-1706-0

Anmerkungen:

Keine Anmerkungen

Sichere Systeme

Modulkürzel:	CSI_SIS	**SPO-Nr.:**	11
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Compulsory Subject	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	English	1 semester	only summer term

Modulverantwortliche(r):	Eggendorfer, Tobias
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Sichere Systeme
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	None

Prüfungsleistungen:

schrP90 - written exam, 90 minutes

Weitere Erläuterungen:
None

Voraussetzungen gemäß SPO:

None

Empfohlene Voraussetzungen:

None

Angestrebte Lernergebnisse:

After attending this module

- participants know primary threats to systems and can suggest appropriate protective measures to mitigate or prevent threats.
- participants can analyze existing systems regarding their IT security and propose suitable measures to increase protection.
- the participants can understand and evaluate basic and advanced concepts of IT security for operating systems.
- the participants can understand and evaluate basic and advanced access concepts and authorization concepts and apply them to specific systems.
- students know relevant standards and can select suitable measures to implement the standards.

Inhalt:

- Threats to operating systems
- Basics of security for operating systems
- Authentication (PAM, LDAP, Kerberos)

- Authorization concepts (Unix, ACLs, capabilities)
- Security architectures and security mechanisms for operating systems (memory management, file management, scheduling, I/O, energy management, secure boot, authenticated bott, TPM)
- Hardening of systems
- Relevant standards
- System examples (SEL4, KataOS, SELinux)

Literatur:

- ADKINS, Heather und andere, March 2020. *Building secure and reliable systems: Best practices for designing, implementing, and maintaining systems*. F. Auflage. Beijing ; Boston ; Farnham ; Sebastopol ; Tokyo: O'Reilly. ISBN 978-1-492-08312-2
- ANDERSON, Ross, 2020. *Security engineering: a guide to building dependable distributed systems* [online]. Indianapolis: Wiley PDF e-Book. ISBN 978-1-119-64468-2, 978-1-119-64283-1. Verfügbar unter: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119644682.

Anmerkungen:

None

Angewandte Mathematik für IT-Sicherheit

Modulkürzel:	CSI_MIS	**SPO-Nr.:**	12
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	3
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Krüger, Max
Leistungspunkte / SWS:	6 ECTS / 5 SWS
Arbeitsaufwand:	Kontaktstunden: 59 h Selbststudium: 91 h Gesamtaufwand: 150 h
Lehrveranstaltungen des Moduls:	12.1: Angewandte Mathematik für IT-Sicherheit 12.2: Übung zu Angewandte Mathematik für IT-Sicherheit
Lehrformen des Moduls:	12.1: SU - seminaristischer Unterricht 12.2: Ü - Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

12.1: schrP90 - schriftliche Prüfung, 90 Minuten
12.2: O - Ohne Leistungsnachweis

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Dieses Modul dient ...

- dem Ausbau des Verständnisses der mathematischen und statistischen Grundlagen der IT-Sicherheit und
- der Vorbereitung auf weiterführende Fächer im Bereich der IT-Sicherheit anhand von ausgewählten Themen aus der und Zahlentheorie, Kryptologie und Statistik.

Nachdem das Modul erfolgreich absolviert wurde ...

- haben die Studierenden Kenntnis von den grundlegenden zahlentheoretischen, kryptologischen und statistischen Begriffen und Notationen, Eigenschaften und Zusammenhängen sowie Algorithmen und ausgewählten Anwendungen.
- können die Studierenden die Begriffe, Zusammenhänge und Algorithmen am Beispiel erläutern und verstehen deren wesentliche Funktionsweisen.

- verstehen die Studierenden die Bedeutung und den Nutzen bei der Beschreibung und Behandlung von Anwendungsproblemen.
- lösen die Studierenden eigenständig typische Aufgabenstellungen.
- erkennen die Studierenden bei der Bearbeitung von Anwendungsproblemen auftretende, grundlegende mathematische Problemstellungen und lösen diese mit geeigneten Verfahren.
- führen die Studierenden einfache mathematische Beweise aus.
- hinterfragen die Studierenden Ergebnisse kritisch hinsichtlich ihrer mathematischen Korrektheit.
- prüfen und beurteilen die Studierenden Ergebnisse kritisch hinsichtlich ihrer Aussage für die zugrunde liegenden Anwendungsprobleme.

Inhalt:

Elementare Zahlentheorie:

- Grundlagen, natürliche, ganze und Primzahlen
- Primfaktorzerlegung und Eigenschaften von Primzahlen
- Euklidischer Algorithmus
- Teilbarkeit und Kongruenz
- Lineare Diophantische Gleichungen
- chinesischer Restsatz
- Satzgruppe von Fermat

Einführung in die Kryptologie

- Ausgewählte Grundlagen der Kryptographie
- Ausgewählte Grundlagen der Kryptoanalyse

Statistik:

- Merkmale, Stichproben, tabellarische und grafische Darstellungen, Lage- und Streuungsmaße,
- Korrelation und Regression
- Zufallsexperimente und Ereignisse
- Wahrscheinlichkeiten und Wahrscheinlichkeitsrechnung,
- Bedingte Wahrscheinlichkeiten
- Zufallsvariablen, Wahrscheinlichkeitsverteilungen und Normalverteilung
- Schätztheorie: Grenzwertsätze, Schätzfunktionen und Konfidenzintervalle
- Testtheorie: Parameter-, Anpassungs- und Unabhängigkeitstests

Literatur:

- FAHRMEIR, Ludwig, HEUMANN, Christian, KÜNSTLER, Rita, PIGEOT, Iris, TUTZ, Gerhard, 2016. *Statistik: der Weg zur Datenanalyse* [online]. Berlin ; Heidelberg: Springer Spektrum PDF e-Book. ISBN 978-3-662-50372-0. Verfügbar unter: https://doi.org/10.1007/978-3-662-50372-0.
- STROTH, Gernot, WALDECKER, Rebecca, 2019. *Elementare Algebra und Zahlentheorie* [online]. Cham: Birkhäuser PDF e-Book. ISBN 978-3-030-25298-4. Verfügbar unter: https://doi.org/10.1007/978-3-030-25298-4.
- ERTEL, Wolfgang und Ekkehard LÖHMANN, 2020. *Angewandte Kryptographie*. 6. Auflage. München: Hanser. ISBN 978-3-446-46353-0

Anmerkungen:

Keine Anmerkungen

Netzwerke

Modulkürzel:	FFI_NW	**SPO-Nr.:**	13
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	3
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Jarschel, Michael
Leistungspunkte / SWS:	7 ECTS / 6 SWS
Arbeitsaufwand:	Kontaktstunden: 70 h Selbststudium: 105 h Gesamtaufwand: 175 h
Lehrveranstaltungen des Moduls:	13.1: Netzwerke 13.2: Praktikum Netzwerke
Lehrformen des Moduls:	13.1: SU/Ü - seminaristischer Unterricht/Übung 13.2: Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

13.1: schrP90 - schriftliche Prüfung, 90 Minuten

13.2: LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:

Erfolgreiches Bestehen des integrierten Praktikums mittels Durchführung von mindestens 7 Versuchen.

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung sind die Studierenden in der Lage,

- die wesentlichen Bestandteile und Aufgaben von Rechner- bzw. Kommunikationsnetzen zu benennen.
- den Unterschied zwischen Leitungs- und Paketvermittlung zu erklären und passende Einsatzfelder zu benennen.
- die Aufgaben und Zusammenhänge zwischen den einzelnen Schichten des TCP/IP-Schichtenmodells für Rechnerkommunikation zu erklären.
- die Leistung gängiger Übertragungstechnologien wie Ethernet und WLAN basierend auf Ihrem erworbenen Wissen zu Zugriffsverfahren einzuschätzen.
- die Allokation von IP-Adressen in einem Netz zu planen und zu strukturieren.
- Routing-Algorithmen anzuwenden und mit Routing-Protokollen in Verbindung zu bringen.

- die Mechanismen der Transportschicht, insbesondere zur verlässlichen Übertragung, Flusskontrolle und Überlastkontrolle zu erklären.
- eine Auswahl des für ihre Anwendung geeigneten Applikations- bzw. Transportschichtprotokolls zur Datenübertragung zu treffen.

Inhalt:

1. Rechnernetze und das Internet
- Aufbau des Internets als Netz von Netzen
- Der Netzzugangsbereich
- Das Kernnetz
- Kenngrößen von paketvermittelten Netzen
- Das TCP/IP Protokollschichten Modell
- Entwicklungsgeschichte des Internets

2. Grundlagen der Bitübertragung.
- Unterschied zwischen Symbol- und Bitübertragung
- Leitungscodierung
- Arten der Signalmodulation
- Übertragungsmedien (elektrisch, optisch, Funk)
- DSL und Kabelzugangsnetze

3. Die Sicherungsschicht und Local Area Network (LANs)
- Fehlererkennung und -korrektur
- Medienzugriffsverfahren
- Multiple-Access Protokolle (Ethernet/WLAN)
- verbindungsorientierte Übertragung von Datenpaketen (MPLS)

4. Die Vermittlungsschicht (Datenpfad)
- Unterscheidung Datenpfad/Kontrollebene
- Bestandteile des Datenpfades innerhalb eines Routers (Ports, Warteschlangen, Fabric)
- IP Datagramme: Struktur und Aufgaben
- IP Adressen: IPv4 Adressierung
- Network Adress Translation
- IP Version 6
- Alternativer Ansatz: Software Defined-Networking

5. Die Vermittlungsschicht (Kontrollebene)
- Routing Protokolltypen: Distance Vector & Link State
- Routing innerhalb eines autonomen Systmen: Das OSPF Protokoll
- Routing zwischen autonomen Systemen: Das BGP Protokoll
- Die Kontrollebene im Fall von Software Defined Networking Ansätzen
- Das ICMP Protokoll

6. Die Transportschicht
- Verbindungs-Multiplexing und Demultiplexing
- Verbindungsloser Transport: Das UDP Protokoll
- Prinzipien von verlässlicher Datenübertragung
- Verbindungsorientierter Transport: Das TCP Protokoll
- Prinzipien der Überlastkontrolle
- TCP Überlastkontrolle
- Neue Entwicklungen: QUIC

7. Die Applikationsschicht

- Beispiele vernetzter Anwendungen
- Architekturen vernetzter Anwendungen
- Das Web und HTTP
- SMTP
- Das Domain Name System (DNS) zur Namensauflösung
- Peer-to-peer Applikationen
- Video-Streaming und Content Distribution Networks (CDNS)
- Programmieren mit TCP- #svhs#amp## UDP Sockets

Literatur:

- KUROSE, James F. und Keith W. ROSS, 2022. *Computer networking: a top-down approach*. E. Auflage. Harlow: Pearson. ISBN 978-1-292-40546-9, 1-292-40546-5
- TANENBAUM, Andrew S., Nick FEAMSTER und David WETHERALL, 2021. *Computer networks*. s. Auflage. Harlow: Pearson. ISBN 978-1-292-37406-2

Anmerkungen:

Keine Anmerkungen

Softwaresicherheit & Security Testing

Modulkürzel:	CSI_SOS	**SPO-Nr.:**	14
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	3
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Softwaresicherheit & Security Testing
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Das Modul "Softwaresicherheit & Security Testing" zielt darauf ab, die Studierenden mit Techniken der Software-Sicherheit und Security-Testing-Verfahren vertraut zu machen. Dabei liegt der Fokus auf den technischen Verfahren der Softwaresicherheit.

Die Studierenden sollen in der Lage sein, sichere Software zu entwickeln und bestehende Software auf Sicherheitslücken zu überprüfen. Sie erlernen Techniken und Strategien zur Sicherstellung der Code-Qualität, einschließlich statischer Code-Analyse und manueller Reviews.

Inhalt:

Die Inhalte der Vorlesung betrachten die technischen Aspekte der Software-Sicherheit. Diese um fassen unter anderem:

Sicheres Programmieren:

- Sicherheitslücken: Die Studenten werden in sicheres Programmieren eingeführt, indem sie lernen, wie man gängige Sicherheitslücken umgeht und Code so schreibt, dass die Auswirkungen von Sicherheitslücken begrenzt sind. Die Auswahl der betrachteten Sicherheitslücken orientiert sich an Listen wie der OWASP Top 10 oder der SANS Top 25.
- Sicherheit von Programmiersprachen: Die Studierenden lernen die Eigenschaften verschiedener Programmiersprachen bezüglich der Softwaresicherheit kennen.

Security Testing:

- Pentesting: In diesem Teil des Moduls lernen die Studierenden, wie sie Penetrationstests durchführen, um Schwachstellen in Software und Systemen zu identifizieren.
- Source Code Reviews: Die Studierenden lernen, wie man Source Code Reviews effizient durchführt (z.B. mittels eines risikorieniternten Ansatzes), um die Sicherheit des Codes zu beurteilen und potenzielle Sicherheitslücken zu identifizieren.
- Statische Code-Analyse: Hier lernen die Studierenden, wie man Werkzeuge zur statischen Code-Analyse verwendet, um potenzielle Sicherheitslücken und Code-Qualitätsprobleme zu identifizieren.
- Manuelles Review: Die Studierenden werden in der manuellen Überprüfung von security-relevanten Dokumenten geschult.
- Security Assessment: Die Studierenden werden in die Methoden der Security Assessment eingeführt, um das allgemeine Sicherheitsniveau von Software und Systemen zu bewerten.
- Relevante Standards: Die Studierenden werden in die relevanten Standards in der Software-Sicherheit eingeführt.

Literatur:

- KOHNFELDER, Loren, 2021. *Designing secure software: a guide for developers*. F. Auflage. San Francisco: No Starch Press. ISBN 978-17185-0192-8
- JOHNSSON, Dan Bergh und andere, 2019. *Secure by design*. Shelter Island, NY: Manning. ISBN 978-1-61729-435-8
- FAIRCLOTH, Jeremy, 2017. *Pentesting mit Open Source: professionelle Penetrationstests mit kostenloser und quelloffener Software : Schlüsseltechniken für jedes Testfeld durch praxisnahe Beispiele verstehen und anwenden : alle gängigen Open-Source-Tools für Penetrationstests ausführlich erklärt : eigenes Labor für Penetrationstests kostengünstig einrichten*. Haar bei München: Franzis. ISBN 978-3-645-60545-8, 3-645-60545-2
- KIM, Peter, 2018. *The Hacker Playbook 3: Practical Guide To Penetration Testing*. ISBN 978-1980901754

Anmerkungen:

Keine Anmerkungen

Software-Design, Software-Architektur und Datenbanken

Modulkürzel:	FFI_SWDDBS	**SPO-Nr.:**	15
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	3
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Cato, Patrick
Leistungspunkte / SWS:	7 ECTS / 6 SWS
Arbeitsaufwand:	Kontaktstunden: 70 h Selbststudium: 105 h Gesamtaufwand: 175 h
Lehrveranstaltungen des Moduls:	15.1: Software-Design, Software-Architektur und Datenbanken 15.2: Praktikum Software-Design, Software- Architektur und Datenbanken
Lehrformen des Moduls:	15.1: SU/Ü - seminaristischer Unterricht/Übung 15.2: Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

15.1: schrP90 - schriftliche Prüfung, 90 Minuten

15.2: LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:

Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Software-Design:

Nach Besuch des Modules

- verstehen die Studierenden Software als Teil eines Systems.
- verstehen die Studierenden die Grundzüge des Software-Systemdesigns.
- kennen die Komplexität von Software-Systemen und von Software-Modulen.
- können die Studierenden die verschiedenen Anforderungsebenen (Systemanforderungen -> Softwareanforderungen -> Design) und deren Unterschiede erläutern.
- können die Studierenden den Zusammenhang zwischen Entwicklungsaufwand und Komplexität (Software Design) erklären.

- kennen die Studierenden die Herausforderungen für die Wiederverwendung von Software - Software Baukasten über Projekte hinweg.

Datenbanksysteme:

Die Studierenden kennen die grundlegenden Prinzipien und Konzepte relationaler Datenbanksysteme und können diese als zentrale fachliche und technologische Infrastruktur-Komponenten zur Datenhaltung in den Kontext unternehmensspezifischer Informationssysteme einordnen.

Sie sind mit den Grundlagen der Datenmodellierung, des Datenbankentwurfs und der Datenintegrität vertraut und in der Lage,

- die wichtigsten hiermit verbundenen Konzepte und Abstraktionsmechanismen zu beschreiben.
- abzuwägen, ob und wie diese zur Umsetzung konkreter fachlicher Anforderungen genutzt werden können.
- (Datenbank-) Schemata zu erstellen.
- Anfrage- bzw. Änderungsoperationen in der Relationenalgebra und SQL zu formulieren.

Basierend auf der Bedeutung und den Prinzipien eines Datenbanksystems verstehen die Studierenden das grundlegende Zusammenspiel von betrieblichen Anwendungssystemen und Datenbanksystemen.

Inhalt:

Software-Design:

- Software als Teil eines Systems -Systemdesign
- Software-Komplexitätsbewertung auf Systemebene und Modulebene
- Anforderungsebenen (Systemanforderungen -> Softwareanforderungen -> Design)
- Systemdesign - Software-Zuweisung an Steuergeräte
- Entwicklung eines verteilten Systems - Zusammenarbeit mit Lieferanten
- Partitionierung von Software
- Wiederverwendung von Software - Software Baukasten über Projekte hinweg Schnittstellung - ICD Interface Control Document

Datenbanksysteme:

- Grundlagen von Datenbanksystemen: Historie, Konzepte und Architektur; 3-Schichten-Modell und Datenunabhängigkeit
- Konzeptioneller (fachlicher) Datenbankentwurf und Entity-Relationship-Modell
- Datenintegrität und Integritätsbedingungen
- Relationales Datenmodell und Relationenalgebra
- Relationaler Datenbankentwurf und Normalformen
- SQL
- Transaktionen und Transaktionsmanagement
- Physische Datenorganisation

Literatur:

- KEMPER, Alfons und André EICKLER, 2015. *Datenbanksysteme: eine Einführung*. 10. Auflage. Berlin ; Boston: de Gruyter Oldenbourg. ISBN 978-3-11-044375-2
- UNTERSTEIN, Michael, MATTHIESSEN, Günter, 2012. *Relationale Datenbanken und SQL in Theorie und Praxis* [online]. Berlin [u.a.]: Springer Vieweg PDF e-Book. ISBN 978-3-642-28985-9, 978-3-642-28986-6. Verfügbar unter: https://doi.org/10.1007/978-3-642-28986-6.
- ELMASRI, Ramez und Sham NAVATHE, 2009. *Grundlagen von Datenbanksystemen*. 3. Auflage. München [u.a.]: Pearson Studium. ISBN 978-3-86894-012-1, 3-86894-012-X
- VOSSEN, Gottfried, 2008. *Datenmodelle, Datenbanksprachen und Datenbankmanagementsysteme*. 5. Auflage. München [u.a.]: Oldenbourg. ISBN 3-486-27574-7, 978-3-486-27574-2

Anmerkungen:

Keine Anmerkungen

Web-Technologien

Modulkürzel:	CSI_WEB	**SPO-Nr.:**	16
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Compulsory Subject	3
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	English	1 semester	only winter term

Modulverantwortliche(r):	Eggendorfer, Tobias
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Web-Technologien
Lehrformen des Moduls:	SU/Ü - lecture with integrated exercises
Verwendbarkeit für andere Studiengänge:	None

Prüfungsleistungen:

schrP90 - written exam, 90 minutes

Weitere Erläuterungen:
None

Voraussetzungen gemäß SPO:

This module can only be taken if the second study section has been achieved. For this purpose, at least 42 credit points (ECTS) from the first study section must be recorded.

Empfohlene Voraussetzungen:

None

Angestrebte Lernergebnisse:

This lecture provides an introduction to commonly used technologies in web applications and web services. Students will be able to write their own web applications and web services. They will be able to analyze web applications

Inhalt:

1. WWW Fundamentals (design principles, protocols like HTTP(S), DNS)
2. Client-side technologies (ISGML, XML, HTML, XHTML, HTML5, CSS, JavaScript, DOM,...)
3. Server-side technologies (session management, PHP, AJAX, NodeJS, APIs, Cookies...)
4. Design of web applications and web services (REST, MVC, ...)
5. Legal issues
6. SEO

Literatur:
Will be specified at the beginning
Anmerkungen:
None

Ethical Hacking Praktikum

Modulkürzel:	CSI_HAC	**SPO-Nr.:**	17
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	4
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Eggendorfer, Tobias
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Ethical Hacking Praktikum
Lehrformen des Moduls:	Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Hilfreich sind erste Erfahrungen mit Linux / Unix sowie die Kenntnisse von Webtechnologien, wie sie u.a. in der Vorlesung Web-Technologien im 2. Semester vermittelt werden. Weiterhin die Teilnahme an der Vorlesung Software-Security und Testing im 2. Semester.

Angestrebte Lernergebnisse:

In diesem Modul erweitern die Studierenden ihre Kenntnisse aus dem Module Software-Security und -Testing durch ein umfassendes Praktikum.

Die Studierenden sammeln im Praktikum Erfahrung mit Angriffen auf Web-Anwendungen und auf reguläre Programme. Dadurch lernen die Studierende typische Sicherheitslücken und deren Vermeidung kennen.

Sie können in der Folge selbständig Systeme auf Sicherheit evaluieren, kennen gängige Sicherheitsprobleme und können ihr Wissen auf weitere Systeme übertragen.

Zusätzlich zu Angriffen auf Web-Anwendungen und reguläre Programme können im Praktikum auch Angriffe auf Netzwerkgeräte, IoT-Geräte und vergleichbare Systeme als ergänzende Lehr-Lern-Inhalte thematisiert werden.

Inhalt:

Angriffe auf Web-Anwendungen, dazu gehören u.a.

- SQL-Injection
- HTML-Injection
- XSS
- XSRF
- XPath-Injection
- LDAP-Injection
- Shell-Command-Injection / Remote-Command-Injection

Angriffe auf reguläre Programme, u.a.

- Buffer-Overflow
- Integer-Overlfow
- Off-By-One
- Out-of-bounds-read
- Format-String-Schwachstellen

Die Liste ist exemplarisch zu verstehen, die Zielsetzung des Praktikums ist, sowohl an "künstlichen" Lernumgebungen als auch an realer Software-Praktikumsaufgaben zu konstruieren, um so ein möglichst breites Spektrum an Sicherheitsproblemen abzudecken.

Literatur:

Wird zu Beginn bekannt gegeben

Anmerkungen:

Keine Anmerkungen

Protokolle der Netzsicherheit

Modulkürzel:	CSI_PNS	**SPO-Nr.:**	18
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	4
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Heinl, Patrizia
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Protokolle der Netzsicherheit
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- können Studierende Grundbegriffe der Kryptologie benennen und definieren.
- besitzen Studierende ein grundlegendes Verständnis symmetrischer und asymmetrischer kryptografischer Verfahren.
- sind Studierende mit den wesentlichen Eigenschaften kryptografischer Protokolle vertraut.
- beherrschen Studierende spezifische Anforderungen an sichere Gruppenkommunikation sowie Konzepte der Zugriffskontrolle.
- kennen und verstehen Studierende Sicherheitsprotokolle der Datensicherungsschicht, die IPsec-Sicherheitsarchitektur sowie Sicherheitsprotokolle der Transportschicht.
- verstehen Studierende Aspekte der sicheren drahtlosen und mobilen Kommunikation.
- sind die Studierenden befähigt, sich selbstständig vertiefende Spezialkenntnisse anzueignen.

Inhalt:

- Zentrale Begriffe und Grundlagen der Kommunikationssicherheit, inkl. Bedrohungen und Sicherheitsanalyse für Netze
- Grundlagen der Kryptologie
- Symmetrische und asymmetrische kryptografische Verfahren
- Kryptografische Protokolle
- Sichere Gruppenkommunikation
- Zugriffskontrolle
- Sicherheitsprotokolle der Datensicherungsschicht
- Die IPsec-Sicherheitsarchitektur
- Sicherheitsprotokolle der Transportschicht
- Grundlagen der sicheren drahtlosen und mobilen Kommunikation

Literatur:

- FORD, Warwick, 2008. *Computer Communications Security - Principles, Standard Protocols and Techniques*. ISBN 978-0137994533
- STALLINGS, William, 2023. *Cryptography and network security: principles and practice*. E. Auflage. Harlow, United Kingdom: Pearson. ISBN 978-1-292-43748-4, 1-292-43748-0
- SCHÄFER, Günter und Michael ROßBERG, 2014. *Netzsicherheit*. 2. Auflage. Heidelberg: dpunkt.verlag. ISBN 978-3-86490-115-7

Anmerkungen:

Die Folien zur Vorlesung sind auf Englisch. Unterrichtssprache ist Deutsch.

Security Architektur & Security Engineering

Modulkürzel:	CSI_SAS	**SPO-Nr.:**	19
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	4
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	7 ECTS / 6 SWS
Arbeitsaufwand:	Kontaktstunden: 70 h Selbststudium: 105 h Gesamtaufwand: 175 h
Lehrveranstaltungen des Moduls:	19.1: Security Architektur & Security Engineering 19.2: Praktikum zu Security Architektur & Security Engineering
Lehrformen des Moduls:	19.1: SU/Ü - seminaristischer Unterricht/Übung 19.2: Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

19.1: schrP90 - schriftliche Prüfung, 90 Minuten
19.2: LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach der erfolgreichen Teilnahme am Modul

- verfügen die Studierenden über grundlegende Kenntnisse über den Security Development Lifecycle in Softwareprojekten und können einen entsprechenden Lebenszyklus für eigene Projekte definieren, durchführen und aufrechterhalten.
- können Studierende den Reifegrad von Security Engineering Prozessen anhand von gängigen Modellen einschätzen.
- können Studierende Security Requirements für eigene Projekte strukturiert ableiten.
- kennen die Studierenden Designprinzipen und Bausteine für sichere IT-Systeme und können diese in eigenen Projekten anwenden.
- erlangen die Studenten durch die Veranstaltung vertiefte Kenntnisse darüber, welche Techniken des Softwareengineering im besonderen Maße auf die Sicherheit aktueller Software abzielen und wie sicherheitsrelevante Schnittstellenrisiken vermieden werden.

Inhalt:

- Security Development Lifecycle, z.B. Microsoft SDL for Agile, DevSecOps
- Security Maturity Models
- Security Requirements Engineering
- Model-based Security
- Designprinzipien wie z.B. Zero Trust Architekturen
- Bausteine für Sicherheitsarchitekturen, z.B. Identity Management Architekturen, Zertifikate und PKIs
- Relevante Standards

Literatur:

- ANDERSON, Ross, 2020. *Security engineering: a guide to building dependable distributed systems* [online]. Indianapolis: Wiley PDF e-Book. ISBN 978-1-119-64468-2, 978-1-119-64283-1. Verfügbar unter: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119644682.
- ADKINS, Heather und andere, 2020. *Building secure and reliable systems: best practices for designing, implementing, and maintaining systems*. F. Auflage. Beijing: O'Reilly. ISBN 978-1-492-08309-2
- FORD, Neal, Mark RICHARDS und Pramod J. SADALAGE, October 2021. *Software architecture: the hard parts ; modern trade-off analysis for distributed architectures*. F. Auflage. Beijing ; Boston ; Farnham ; Sebastopol ; Tokyo: O'Reilly. ISBN 978-1-492-08689-5

Anmerkungen:

Bonuspunkteregelung:

Für diese Vorlesung werden Bonuspunkte gemäß APO §25 Absatz (2) vergeben. Im Laufe des Semesters können die Studierenden jede Woche eine Aufgabe lösen und durch ein erfolgreiches Bearbeiten jeweils 1/2 Bonuspunkt erwerben. Dadurch kann ein Bonus von maximal 5 Bonuspunkten bzw. 5 % der in der Klausur vergebenen Punkte erreicht werden. Die genauen Bedingungen sind im Moodle-Kursraum zur Veranstaltung hinterlegt (Link: https://moodle.thi.de/course/view.php?id=9410).

Projekt-, Qualitäts- und Risikomanagement

Modulkürzel:	CSI_PQRM	**SPO-Nr.:**	20
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	4
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Projekt-, Qualitäts- und Risikomanagement
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach dem erfolgreichen Besuch der Lehrveranstaltung

- haben die Studierenden die Basis-Kompetenzen für das Management kleiner und mittlerer Projekte im industriellen/technischen Umfeld.
- sind den Hörern dieser Vorlesung die relevanten Schritte in der Vorphase der Planungen eines Projekts bekannt und anhand von Gruppenarbeiten auch eingeübt.
- hatten sie im Rahmen der Gruppenarbeiten die Gelegenheit, ihre Ergebnisse in einer kurzen Präsentation vorzustellen und zu diskutieren.
- sind sie befähigt, einen korrekten Start (Kick-off) eines Projekts zu organisieren und alle dafür erforderlichen Vorarbeiten und Analysen zu erledigen.
- sind die Studierenden in der Lage, ein Projekt im Detail zu planen und haben dies auch an einem realen Fall durchgeführt.
- kennen sie mehrere Methoden zur Analyse eines laufenden Projekts und zur Erstellung von Trendaussagen über den Fortschritt des Projekts.

- verstehen sie relevante Zusammenhänge im Ablauf von Projekten und können Entscheidungen für die weitere Steuerung eines Projekts auf fundierte Methoden setzen.
- sind ihnen auch neue Ansätze und Methoden des agilen Projektmanagements bekannt.
- haben sie auch eine Vertiefung der Basis-Techniken zum wissenschaftlichen Arbeiten erzielt.

Inhalt:

1. Grundlagen:
   - Definition Projekt, Projektdreiecks (Zeit, Budget, Leistung)
   - Typische Projektorganisationen
2. Vorphase eines Projekts:
   - Vorgehensmodelle
   - Zieldefinition
   - Stakeholder-Analyse / -Management
   - Risiko-Analyse / -Management
   - Scope und Kick-off
   - Gruppenarbeiten zur Vertiefung
3. Planung eines Projekts
   - Projektstrukturplan, Ablaufplan / Netzpläne
   - Aufwandschätzungen
   - Ressourcenplanung
4. Durchführung eines Projekts
   - Fortschritt- und Trend-Analysen
   - Kosten / Berichterstattung
   - Controlling und Änderungsmanagement
5. Agile Methoden des Projektmanagements
   - Idee und Ansatz agiler Methoden im Projektmanagement
   - Vorgehen und Rollen bei Scrum

Literatur:

- MEYER, Helga, REHER, Heinz-Josef, 2020. *Projektmanagement: von der Definition über die Projektplanung zum erfolgreichen Abschluss* [online]. PDF e-Book. ISBN 978-3-658-28763-4. Verfügbar unter: https://doi.org/10.1007/978-3-658-28763-4.
- SCHELLE, Heinz und Roland OTTMANN, 2014. *Projekte zum Erfolg führen: Projektmanagement systematisch und kompakt*. 7. Auflage. München: Dt. Taschenbuchverl.. ISBN 978-3-423-50937-4, 3-423-50937-6
- SEIBERT, Siegfried, 2006. *Technisches Management: Innovationsmanagement, Projektmanagement, Qualitätsmanagement*. B. Auflage. Groß-Umstadt: SMP. ISBN 3-519-06363-8
- BOHINC, Tomas, 2014. *Grundlagen des Projektmanagements: Methoden, Techniken und Tools für Projektleiter*. 5. Auflage. Offenbach am Main: GABAL. ISBN 978-3-86936-121-5, 3-86936-121-2 https://www.wiso-net.de/document/GABA,AGAB__9783956238512240
- SUTHERLAND, Jeff und Jan W. HAAS, 2015. *Die Scrum-Revolution: Management mit der bahnbrechenden Methode der erfolgreichsten Unternehmen*. [Frankfurt am Main]: Campus Frankfurt ; New York. ISBN 978-3-593-42447-7

Anmerkungen:

Keine Anmerkungen

Recht für IT-Sicherheit und Datenschutz

Modulkürzel:	CSI_RID	**SPO-Nr.:**	21
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	6
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	3 ECTS / 2 SWS
Arbeitsaufwand:	Kontaktstunden: 24 h Selbststudium: 51 h Gesamtaufwand: 75 h
Lehrveranstaltungen des Moduls:	Recht für IT-Sicherheit und Datenschutz
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung sind die Studierenden in der Lage,

- wichtige Bereiche des Rechts mit Bezug zu Cybersicherheit und Datenschutz zu beschreiben.
- in ihrem Berufsfeld rechtlich relevante Probleme zu erkennen.
- Lösungsansätze zu erarbeiten und diese in der Praxis umzusetzen und anzuwenden.

Inhalt:

- Rechtliche Grundlagen
- Grundrecht auf informationelle Selbstbestimmung, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
- Datenschutzrecht, GDPR (DSGVO)
- Rechtliche Grundlagen für Forensik, Vorfallverfolgung und Strafverfolgung
- Cyberwar-Regulierung

• Ausgesuchte nationale und internationale rechtliche Regelungen mit Bezug zur Cybersicherheit (z.B. KRITIS-Verordnung, Sarbanes-Oxley Act, EU Cybersecurity Act)
Literatur:
• KENJI KIPKER , Dennis, Philipp REUSCH und Steve RITTER, 2023. *Recht der Informationssicherheit: BSIG, EU Cybersecurity Act, DS-GVO*. ISBN 978-3406783395 • TINNEFELD, Marie-Theres und andere, 2024. *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*. 8. Auflage. Berlin: De Gruyter Oldenbourg. ISBN 978-3-11-101830-0, 3-11-101830-X
Anmerkungen:
Keine Anmerkungen

Fachwissenschaftliches Seminar

Modulkürzel:	CSI_FWS	**SPO-Nr.:**	22
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	4
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Heinl, Patrizia
Leistungspunkte / SWS:	3 ECTS / 2 SWS
Arbeitsaufwand:	Kontaktstunden: 24 h Selbststudium: 51 h Gesamtaufwand: 75 h
Lehrveranstaltungen des Moduls:	Fachwissenschaftliches Seminar
Lehrformen des Moduls:	S - Seminar
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

SA - Seminararbeit

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- besitzen die Studierenden die Fähigkeit, sich selbständig spezielle fachliche Kenntnisse zu erarbeiten (Literaturarbeit, Analyse, Schlussfolgerungen) und können diese mithilfe des Einsatzes geeigneter Medien nachvollziehbar im Rahmen eines mündlichen Vortrags präsentieren.
- sind die Studierenden in der Lage, einer fachlichen Präsentation kritisch zu folgen und die Inhalte mit dem Vortragenden fachlich zu diskutieren (Stärkung der kommunikativen Kompetenz).
- haben die Studierenden ihre überfachlichen und kommunikativen Kompetenzen verstärkt.
- können die Studierenden den Inhalt ihrer Präsentation in Form einer kurzen schriftlichen Ausarbeitung darstellen.

Inhalt:

Das fachliche Thema des Seminars wechselt von Kurs zu Kurs. Gegenstand ist zumeist ein studiengangspezifisches Gebiet, zu dem es geeignete Fachliteratur gibt, die zugleich die Basisliteratur für die Vorträge darstellt. Die Literatur wird vom jeweiligen Dozierenden zur Verfügung gestellt.

Im Zuge des Seminars muss jeder Teilnehmende eine Unterrichtseinheit (45 Minuten) über ein Thema gestalten, welches zu Beginn des Semesters per Los oder Wahl zugeteilt wird.

- In der Vorbereitungsphase muss jeder Teilnehmende Literaturrecherchen zum jeweils zugeteilten Thema durchführen und deren Ergebnis in eine Präsentation einarbeiten.
- Diese Präsentation tragen die Teilnehmenden jeweils im Rahmen einer Unterrichtseinheit mündlich vor. Der Vortrag soll ca. 30 Minuten dauern. Die restlichen ca. 15 Minuten der Unterrichtseinheit sind für die Diskussion des Vortrags vorgesehen. Es wird erwartet, dass die jeweiligen Vortragenden in der Diskussionsrunde nicht nur Fragen der anderen Teilnehmenden beantworten, sondern die Diskussionsrunde auch aktiv moderieren, in dem sie im Vorfeld beispielsweise Fragen an die anderen Teilnehmenden vorbereiten.
- Zusätzlich ist eine schriftliche Ausarbeitung über das bearbeitete Thema zu erstellen. Diese Ausarbeitung soll die wesentlichen Inhalte des Vortrags in Prosa zusammenfassen und einen Umfang von ca. 10 Seiten haben.

Detaillierte Hinweise zu Terminen und weiteren Erwartungen hinsichtlich der Gestaltung der Präsentation sowie der schriftlichen Ausarbeitung kommunizieren die jeweiligen Dozierenden zu Beginn des Semesters.

Literatur:

- , . *Literatur wird zu Beginn bekannt gegeben.*.

Anmerkungen:

In diesem Modul besteht Anwesenheitspflicht.

Cloud-Architekturen und -Dienste

Modulkürzel:	FFI_CARCH	**SPO-Nr.:**	23
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	4
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Jarschel, Michael
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Cloud-Architekturen und -Dienste
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung,

- kennen die Studierenden aktuelle Technologien, die die Basis bilden für skalierbare Anwendungen im Web- und Cloud-Kontext.
- kennen die Studierenden Referenzarchitekturen und Architekturstile in verteilten Anwendungen in der Cloud und damit notwendige Dienste zur Orchestrierung der Systemlandschaft.
- kennen die Studierenden den Unterschied zwischen Hypervisor-basierter Virtualisierung und Containerisierung.
- können die Studierenden eine einfache virtualisierte Instanz aufzusetzen.
- können die Studierenden eine (webbasierte) Anwendung über ein Containerformat bereitstellen und eine einfache skalierbare verteilte Anwendung umsetzen und in einer Cloud-Infrastruktur zur Ausführung bringen.

Inhalt:

1. Grundlagen

- Konzepte und Modelle
- Basistechnologien
- Containerisierung

2. Mechanismen des Cloud Computing

- Infrastruktur
- Cloud-spezifische Mechanismen
- Zugangsmechanismen
- Management

3. Cloud Computing Architekturen

- Basisarchitekturen
- Fortgeschrittene Konzepte
- Spezielle Architekturen

4. Arbeiten mit Clouds

- Auswahl des Bereitstellungsmodells
- Kostenmetriken
- Service Level Agreements (SLAs) und Metriken

Literatur:

- ERL, Thomas und Eric Barceló MONROY, 2024. *Cloud Computing: concepts, technology, security & architecture*. s. Auflage. Hoboken, NJ: Pearson. ISBN 978-0-13-805225-6, 0-13-805225-5

Anmerkungen:

Keine Anmerkungen

Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit

Modulkürzel:	CSI_GKI	**SPO-Nr.:**	24
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	6
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Heinl, Patrizia
Leistungspunkte / SWS:	7 ECTS / 6 SWS
Arbeitsaufwand:	Kontaktstunden: 70 h Selbststudium: 105 h Gesamtaufwand: 175 h
Lehrveranstaltungen des Moduls:	24.1: Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit 24.2: Praktikum Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit
Lehrformen des Moduls:	24.1: SU/Ü - seminaristischer Unterricht/Übung 24.2: Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

24.1: schrP90 - schriftliche Prüfung, 90 Minuten
24.2: LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- kennen die Studierenden grundlegende Methoden der Künstlichen Intelligenz und können diese Methoden in eigenen Projekten einsetzen.
- kennen die Studierende verschiedene Angriffe auf Methoden der Künstlichen Intelligenz und können diese vermeiden.
- kennen die Studierenden verschiedene Angriffe durch Methoden der Künstlichen Intelligenz und können geeignete Schutzmaßnahmen gegen solche Angriffe ergreifen.
- kennen die Studierenden verschiedenen Anwendungsgebiete für Künstliche Intelligenz in der IT-Sicherheit (z.B. Intrusion Detection).

Inhalt:

- Einführung in die Grundlagen der Künstlichen Intelligenz
- Aktuelle Methoden der Künstlichen Intelligenz (z.B. tiefe neuronale Netze, Transformer, ...)
- Angriffe auf Methoden der Künstlichen Intelligenz und deren Vermeidung, Sicherheit von KI-Modellen
- Angriffe durch Künstliche Intelligenz und Auswirkungen auf das Design sicherer Systeme
- Generierung von Datensätzen für das Training von Künstlicher Intelligenz
- Künstliche Intelligenz in der Cybersicherheit:
  - KI in der Intrusion Detection
  - KI in der Statische Code-Analyse
  - KI in der Threat Intelligence/Security Data Mining
  - KI im Penetration Testing
  - Aktuelle Entwicklungen KI in der Cybersecurity

Literatur:

- HUANG, Ken , Yang WANG und Ben GOERTZEL , . *Generative AI Security*. ISBN 978-3031542510
- MILLER, David J., Zhen XIANG und George KESIDIS, 2024. *Adversarial learning and secure AI*. Cambridge: Cambridge University Press. ISBN 978-1-009-31567-8

Anmerkungen:

Keine Anmerkungen

Incident Response und Netzwerkmonitoring

Modulkürzel:	CSI_IRN	**SPO-Nr.:**	25
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	6
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Heinl, Patrizia
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Incident Response und Netzwerkmonitoring
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- verstehen Studierende die Kill Chain, den Incident Response Lebenszyklus sowie zugehörige Maßnahmen.
- beherrschen Studierende grundlegende Fähigkeiten zur Koordination verschiedener Incident Response Stakeholder.
- sind Studierende mit der Planung der Incident-Response-Readiness vertraut.
- haben Studierende eine Übersicht bekannter Frameworks und Tools für Incident Response.
- sind Studierende in der Lage, Netzwerk-Monitoring sinnvoll in die Incident Response Planung zu integrieren

Inhalt:

- Kill Chain und Incident Response Lifecycle
- Übersicht und Interaktion verschiedener Incident Response Stakeholder

- Organisatorische Aspekte von Incident Response
- Vorbereitende Maßnahmen
- Detektive Maßnahmen, z. B.
  - Intrusion Detection Systeme (IDS)
  - Honeypots und Honeynets
- Reaktive Maßnahmen, z. B.
  - Intrusion Prevention Systeme (IPS)
- Wiederherstellende Maßnahmen
- Übersicht verschiedener forensischer Teilgebiete, z. B. Netzwerkforensik
- Systematischer Einsatz von Threat Intelligence und Security Information und Event Management (SIEM)
  - Indicators of Compromise (IoCs)
  - Tactics, Techniques, and Procedures (TTP)

Literatur:

- JOHANSEN, Gerard, June 2020. *Digital forensics and incident response: incident response techniques and procedures to respond to modern cyber threats*. S. Auflage. Birmingham ; Mumbai: Packt. ISBN 978-1-83864-408-6

Anmerkungen:

Keine Anmerkungen

Sichere Netzwerkarchitekturen und Sicherheit vernetzter Anwendungen

Modulkürzel:	CSI_SNT	**SPO-Nr.:**	26
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	6
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Sichere Netzwerkarchitekturen und Sicherheit vernetzter Anwendungen
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach einem Besuch der Modulveranstaltungen und aktiver Teilnahme am Kurs

- kennen Studierende typische Einsatzszenarien von Firewalls und anderen Schutzkomponenten für Netzwerke und können für eigene Netzwerke sinnvolle Sicherheits-Architekturen entwerfen.
- kennen Studierende typische Angriffsmöglichkeiten auf Clouds und können Schutzmaßnahmen einsetzen, um diesen wirksam zu begegnen.
- kennen Studierende typische Angriffe auf Web-Anwendungen und Apps und wissen, wie man diese vermeidet.
- sind Studierende in der Lage, eigene Web-Anwendungen und Apps gegen Angriffe zu schützen.
- haben Studierende die Kompetenz, das Sicherheitsniveau von Sicherheitsarchitekturen einzuschätzen und durch geeignete Maßnahmen anzuheben.

Inhalt:

- Sicherheitsarchitekturen von Netzwerken (z.B. Firewall-Architekturen)
- Cloud Security

- Angreifermodelle
- Schutzmaßnahmen
- Cloud Computing Security Standards

- IT-Sicherheit von Web-Anwendungen
  - Typische Schwachstellen in Web-Anwendungen
  - Schutzmaßnahmen einschließlich sicherer Kommunikation für Web-Anwendungen (SSL/TLS, HTTPS, etc.)
- App Security
  - Typische Schwachstellen in aktuellen Smartphone-Betriebssystemen
  - Schutzmaßnahmen einschließlich sicherer Kommunikation für Apps
- Sicheres Programmieren für typische Programmiersprachen von Web-Anwendungen und Apps (z.B. JavaScript, Java, PHP, Objective-C, Swift, etc.)
- Security User Experience (Thematisierung verschiedener Usability-Probleme gängiger Anwendungen)

Literatur:

- CRANOR, Lorrie Faith, 2005. *Security and usability: designing secure systems that people can use*. 1. Auflage. Beijing [u.a.]: O'Reilly. ISBN 0-596-00827-9, 978-0-596-00827-7
- CREANE, Brendan und Amit GUPTA, 2021. *Kubernetes security and observability: a holistic approach to securing containers and cloud native applications*. F. Auflage. Beijing ; Boston ; Farnham: O'Reilly. ISBN 978-1-0981-0710-9
- HOFFMAN, Andrew, 2024. *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*. 2. Auflage. Sebastopol: O'Reilly Media. ISBN 978-1-09-814393-0
- THIEL, David, 2016. *iOS application security: the definitive guide for hackers and developers*. San Francisco: No Starch Press. ISBN 978-1-59327-601-0, 1-59327-601-X
- GUNASEKERA, Sheran, 2020. *Android Apps Security: Mitigate Hacking Attacks and Security Breaches* [online]. Berkeley, CA: Apress PDF e-Book. ISBN 978-1-4842-1682-8. Verfügbar unter: https://doi.org/10.1007/978-1-4842-1682-8.

Anmerkungen:

Keine Anmerkungen

Projekt

Modulkürzel:	CSI_PRO	**SPO-Nr.:**	27
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	6
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Projekt
Lehrformen des Moduls:	Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

Proj - Projektarbeit

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls sind die Studierenden in der Lage,

- mindestens eine bestimmte Projektmanagementmethode praktisch einzusetzen (vorzugsweise Scrum oder Kanban).
- konkrete Werkzeuge einzusetzen, die üblicherweise im Rahmen der Durchführung eines IT-Projekts zur Anwendung kommen (IDE, RCS, Ticket-System, Scrum Board).
- mit fachlichen und nicht-fachlichen Problemen umzugehen, die während der Durchführung eines mehrwöchigen Projekts auftreten können.
- eine komplexe fachliche Aufgabenstellung aus dem Bereich der Cybersecurity zu analysieren und über ein Semester hinweg in einem Team erfolgreich zu bearbeiten.
- in unterschiedlicher aber stets angemessener Ausführlichkeit über den Projektfortschritt in mündlicher und/oder schriftlicher Form zu berichten.
- neben fachlichen Problemstellungen auch betriebswirtschaftliche Aspekte eines Projekts zu erkennen und diese zur Gewährleistung des Gesamterfolgs angemessen zu unterstützen.

Inhalt:

Praktische Anwendung einer Projektmanagement-Methode (z.B. Scrum, Kanban)

- Planen von Aufgaben (Tasks) und Aufwandsabschätzung im Team
- Praktische Anwendung von Software-Entwicklungswerkzeugen (IDE, RCS, Ticket System, Scrum Board)
- Arbeiten im Team
- Einsatz von Techniken der agilen Software-Entwicklung: Pair Programming, Test Driven Development, Unit Testing, CI/CD
- Reporting des Projektfortschritts, z.B. Daily Scrum
- Präsentation von Projektergebnissen

Literatur:

- SHORE, James, Wolf-Gideon BLEEK und Tim MÜLLER, 2023. *Die Kunst der agilen Entwicklung: Grundlagen, Methoden und Praktiken*. 1. Auflage. Heidelberg: dpunkt.verlag. ISBN 978-3-96910-866-6, 978-3-96910-867-3
- DRÄTHER, Rolf, Holger KOSCHEK und Carsten SAHLING, 2023. *Scrum - kurz & gut*. 3. Auflage. Heidelberg: o'Reilly. ISBN 978-3-96010-780-4
- WOLF, Henning und Stefan ROOCK, 2021. *Scrum - verstehen und erfolgreich einsetzen*. 3. Auflage. Heidelberg: dpunkt.verlag. ISBN 978-3-96910-538-2

Anmerkungen:

Keine Anmerkungen

Grundlagen der Betriebswirtschaft und des Gründertums

Modulkürzel:	CSI_BWG	**SPO-Nr.:**	28
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	6
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Grundlagen der Betriebswirtschaft und des Gründertums
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

schrP90 - schriftliche Prüfung, 90 Minuten

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls sind die Studierenden in der Lage,

- die wesentlichen Merkmale unternehmensverantwortlichen Handelns zu beschreiben.
- Grundlagen der Globalisierung und der Marktwirtschaft zu verstehen.
- Marktformen und Wirtschaftsräume sowie Absatzpolitik und Marketing Mix zu unterscheiden.
- Unternehmensorganisation und Unternehmensstrukturen zu beschreiben.
- die wesentlichen Merkmale des und Vorgehensweisen im Innnovationsmanagement zu beschreiben.
- Unterschiedliche Führungsstile zu benennen und verschiedene Ausprägungen der Personalorganisation zu erklären.
- die wesentlichen Aspekte des Gründertums wie Grundkenntnisse der Finanzierung, der Buchhaltung und der Investitionsrechnung zu verstehen und im praxisbezogenen Kontext anzuwenden.
- Grundlegende Formen der Material- und Produktionswirtschaft zu benennen.

Inhalt:

Betriebswirtschaftliche Grundlagen des Gründertums:

- Grundbegriffe (Ziele, konstitutive Entscheidungen wie z.B. über Rechtsform sowie Kooperationen, Entscheidungsregeln)
- Grundlagen der Globalisierung und der Marktwirtschaft
- Marktformen und Wirtschaftsräume, Absatzpolitik und Marketing Mix
- Unternehmensorganisation, Unternehmensstrukturen
- Führungsstile und Personalorganisation
- Grundlagen der Material- und Produktionswirtschaft
- Grundkenntnisse der Finanzierung, der Buchhaltung und der Investitionsrechnung
- Innnovationsmanagement (Merkmale und Vorgehensweisen)

Grundlagen Entrepreneurship und Intrapreneurship:

- Entrepreneur / Intrapreneur - Grundlagen
- Konzeptionelle Aspekte – Businessplan, Business Model Canvas, Entrepreneur Marketing, Unternehmenskultur
- Kooperationen – Inkubatoren, Akzeleratoren, Company Builder
- Gründungsfinanzierung

Literatur:

- , . *Allgemeine Betriebswirtschaftslehre*. 9. Auflage. Wiesbaden: Springer. ISBN 978-3-658-27246-3
- , 2024. *Startup Navigator – Das Workbook zur Unternehmensgründung*. 2. Auflage. ISBN 978-3446476066
- , . *Mein Einstieg in die Selbstständigkeit: Existenzgründung Schritt für Schritt erklärt: Unternehmensgründung von der Ideenfindung über den Businessplan bis zum Marketing & vieles mehr*. ISBN 978-3910390102

Anmerkungen:

Keine Anmerkungen

Seminar Bachelorarbeit

Modulkürzel:	CSI_SBA	**SPO-Nr.:**	30.1
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	7
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	3 ECTS / 2 SWS
Arbeitsaufwand:	Kontaktstunden: 0 h Selbststudium: 75 h Gesamtaufwand: 75 h
Lehrveranstaltungen des Moduls:	Seminar Bachelorarbeit
Lehrformen des Moduls:	S - Seminar
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung,

- kennen die Studierenden sowohl formale als auch inhaltliche Anforderungen, die an eine Bachelorarbeit gestellt werden.
- sind die Studierenden mit den grundlegenden wissenschaftlichen Arbeitsmethoden vertraut, die im Rahmen der Erstellung einer Abschlussarbeit zur Anwendung kommen.
- haben die Studierenden ein besseres Verständnis darüber, wie eine Abschlussarbeit aufgebaut ist, wie Zielsetzungen/Hypothesen zu definieren und Erkenntnisse aus der Bearbeitung zu präsentieren sind.
- wissen die Studierenden, wie man eine umfangreiche wissenschaftliche Arbeit strukturiert und prägnant einem breiten Publikum vermitteln kann.
- sind die Studierenden darin geübt, sachlich und objektiv zu argumentieren und mit konstruktiver Kritik umzugehen.

Inhalt:

Einführung / Informationsveranstaltung via Moodle-Online-Kurs "Seminar Bachelorarbeit":

- Wissenschaftlicher Anspruch der Bachelorarbeit
- Prüfungsrechtliche Rahmenbedingungen
- Einführung in die Recherche- und Dokumentationstechniken durch die Hochschulbibliothek Themenfindung
- Individuelle Wahl des Themas und des Betreuers
- Eigenständige Kontaktaufnahme mit Unternehmen und Professoren Einarbeitung
- Individuelle Kontaktaufnahme mit dem betreuenden Dozenten und Themenvorschlag
- Einarbeitung und schriftliche Formulierung der Themenstellung
- Zeitplan für die Bachelorarbeit erstellen und abstimmen
- Gliederung der Bachelorarbeit aufstellen
- Anmeldung der Bachelorarbeit vorbereiten

Literatur:

- , . *Wissenschaftliches Schreiben und Abschlussarbeit in Natur- und Ingenieurwissenschaften : Grundlagen - Praxisbeispiele - Übungen*.
- , . *Die Form der wissenschaftlichen Arbeit : Grundlagen, Technik und Praxis für Schule, Studium und Beruf*.

Anmerkungen:

Keine Anmerkungen

Bachelorarbeit

Modulkürzel:	CSI_BAB	**SPO-Nr.:**	30.2
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	7
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	12 ECTS / 0 SWS
Arbeitsaufwand:	Kontaktstunden: 0 h Selbststudium: 300 h Gesamtaufwand: 300 h
Lehrveranstaltungen des Moduls:	Bachelorarbeit
Lehrformen des Moduls:	BA - Bachelorarbeit
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

BA - Bachelor-Abschlussarbeit

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Voraussetzung für die Ausgabe der Bachelorarbeit ist die erfolgreiche Ableistung des praktischen Studiensemesters.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach der erfolgreichen Erstellung der Bachelorarbeit sind die Studierenden in der Lage,

- ein Problem aus der Cybersicherheit selbstständig und unter Einsatz wissenschaftlicher Methoden zu bearbeiten.
- Anforderungen, alternative Lösungsvorschläge sowie möglicherweise die Ausarbeitung einzelner Lösungsansätze zu bewerten und schriftlich in einer überzeugenden und nachvollziehbaren Weise darzustellen.
- eine umfangreiche Aufgabenstellung durch effektives Zeitmanagement in einem vorgegebenen Zeitrahmen zum Abschluss zu bringen.

Inhalt:

Eine Bachelorarbeit ist der wissenschaftliche Abschluss eines Studiums und Bestandteil der Prüfung. Sie soll zeigen, dass der/die Studierende in der Lage ist, ein Problem aus seinem Studiengang selbstständig und unter Einsatz wissenschaftlicher Methoden zu bearbeiten. Dies umfasst die detaillierte Problemanalyse, die

Identifikation einer geeigneten theoretischen oder experimentellen Lösungsstrategie, die Lösung des Problems im vorgegebenen Zeitraum und die Dokumentation der Ergebnisse.
Literatur:
• GERLACH, Silvio, 2019. *Thesis-ABC: in 31 Tagen zur Bachelorarbeit oder Masterarbeit*. 4. Auflage. Berlin: Studeo Verlag. ISBN 978-3-936875-87-4, 3-936875-87-1
Anmerkungen:
Für Dual-Studierende gilt, dass die Abschlussarbeit gemäß APO §30(5) bei der Dual-Partnerfirma geleistet werden muss.

Kommunikations- und Teamkompetenz

Modulkürzel:	CSI_KOT	**SPO-Nr.:**	31
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	5
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	2 ECTS / 1 SWS
Arbeitsaufwand:	Kontaktstunden: 12 h Selbststudium: 38 h Gesamtaufwand: 50 h
Lehrveranstaltungen des Moduls:	Kommunikations- und Teamkompetenz
Lehrformen des Moduls:	S - Seminar
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung sind die Studierenden in der Lage,

- sich in alltäglichen Situationen des beruflichen Miteinanders angemessen zu verhalten.
- ihre eigene Kommunikations- und Teamkompetenz zu reflektieren und gezielter einzusetzen.
- Konflikte und deren Dynamik zu analysieren.
- zielführende Lösungsansätze im Umgang mit kritischen Situationen und Konflikten zu entwickeln.

Inhalt:

Diskussion von Erwartungen, Befürchtungen, Unsicherheiten und Handlungsempfehlungen im Hinblick auf das bevorstehende Firmenpraktikum

- Einschätzung von Persönlichkeitsprofilen
- Reflexion eigener Stärken und Schwächen
- Einüben verschiedener Kommunikations- und Konfliktlösungstechniken im Rahmen von Gruppenübungen und Rollenspielen

Literatur:
• GAY, Friedbert und Debora KARSCH, 2021. *Das persolog Persönlichkeits-Profil: persönliche Stärke ist kein Zufall*. 43. Auflage. [Offenbach]: GABAL. ISBN 978-3-86936-929-7, 3-86936-929-9
Anmerkungen:
Keine Anmerkungen

Praktikum (18 Wochen)

Modulkürzel:	CSI_PRA	**SPO-Nr.:**	32
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	5
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	26 ECTS / 0 SWS
Arbeitsaufwand:	Kontaktstunden: 0 h Selbststudium: 650 h Gesamtaufwand: 650 h
Lehrveranstaltungen des Moduls:	Praktikum (18 Wochen)
Lehrformen des Moduls:	Pr - Praktikum
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

PB - Praktikumsbericht

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in das praktische Studiensemester ist nur berechtigt, wer alle Prüfungen des ersten Studienabschnitts bestanden und mindestens 20 Leistungspunkte aus Modulen der ersten beiden Semester des zweiten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Die Studierenden können das in den vorhergehenden theoretischen Semestern Gelehrte in der betrieblichen Praxis der Cybersicherheit anwenden und lernen

- grundlegende Konzepte und Methoden des Projekt- und Konfigurationsmanagements kennen.
- die eigene Arbeit zu organisieren und Initiative zu zeigen.
- Ergebnisse zu begründen, schriftlich zu fixieren und zu präsentieren.
- Verantwortlichkeit bei der Systementwicklung im technisch-sicherheitskritischen und ethischen Umfeld zu zeigen.
- projektverantwortlich in Entwicklungsprojekten zu handeln.

Inhalt:
Das praktische Studiensemester des zweiten Studienabschnitts umfasst einen Zeitraum von 18 Wochen und wird durch Lehrveranstaltungen begleitet. Das Praxissemester ist während des Studiums für alle Studierenden zu durchlaufen. Es wird in Unternehmen aus Industrie, Mittelstand und öffentlicher Verwaltung durchgeführt. Es ist ein Bericht anzufertigen. • Auswahl eines geeigneten Unternehmens im In- oder Ausland • Mitarbeit an konkreten betrieblichen Aufgabenstellungen unter Anwendung der erlernten Methoden • Kennenlernen betrieblicher Abläufe und Arbeitsmethoden.
Literatur:
• , . *Die 80 wichtigsten Management- und Beratungstools : Von der BCG-Matrix zu den agilen Tools*. • , . *Scrum think big : Scrum für wirklich große Projekte, viele Teams und viele Kulturen*.
Anmerkungen:
Dual-Studierende müssen gemäß APO §29(3) das Praxissemester bei Ihrem Dual-Unternehmen ableisten.

Nachbereitendes Praxisseminar

Modulkürzel:	CSI_NPS	**SPO-Nr.:**	33
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cybersicherheit (SPO WS 22/23)	Pflichtfach	5
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	2 ECTS / 1 SWS
Arbeitsaufwand:	Kontaktstunden: 12 h Selbststudium: 38 h Gesamtaufwand: 50 h
Lehrveranstaltungen des Moduls:	Nachbereitendes Praxisseminar
Lehrformen des Moduls:	S - Seminar
Verwendbarkeit für andere Studiengänge:	Keine

Prüfungsleistungen:

LN - ohne/mit Erfolg teilgenommen

Weitere Erläuterungen:
Keine

Voraussetzungen gemäß SPO:

Zum Eintritt in den zweiten Studienabschnitt ist lt. §7(1) nur berechtigt, wer mindestens 42 Leistungspunkte aus Modulen des ersten Studienabschnitts erzielt hat.

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung,

- können die Studierenden praktische Arbeiten aus ihrem Berufsfeld analysieren und im Hinblick auf die im Studium gelernten Inhalte bewerten.
- haben die Studierenden ihre Präsentationsfähigkeiten vertieft und können technische und projektbezogene Themen vor einem Publikum referieren und vermitteln.
- sind die Studierenden in der Lage, sich in technische Themen aus der Praxis einzuarbeiten und diese entsprechend aufzubereiten.
- können die Studierenden entsprechende Materialien (PowerPoint-Folien, Handouts) erstellen.
- sind die Studierenden in der Lage, technische Themen in der Gruppe zu diskutieren.
- können die Studierenden in Diskussionen anderen Teilnehmern ein Feedback geben, das sowohl technische als auch präsentationsbezogene und soziale Aspekte umfasst.

Inhalt:

- Präsentation von Kurzreferaten mit anschließender Diskussion der Ergebnisse und ihrer Darstellung

- Verknüpfung der Erfahrungen aus der Praxis mit theoretischen Kenntnissen
- Förderung der sozialen Fähigkeiten durch gruppendynamische Prozesse (Diskussionen, Übungen, Rollenspiele)
- Analyse erfolgreicher Vortragstechniken anhand von Beispielen
- Diskussion über die im Studium gelernten Inhalte und deren Anwendung in der Praxis

Literatur:

- , . *Präsentieren können: Das neue Handbuch für authentische Präsentationen*.
- , . *Mehr Klarheit mit Visualisierung im Business: 36 Tools zum einfachen Visualisieren und Lösen komplexer Aufgaben*.
- , . *Storytelling mit Daten: Die Grundlagen der effektiven Kommunikation und Visualisierung mit Daten*.

Anmerkungen:

Für Dual-Studierende ist eine spezielle Veranstaltung PLV 2 eingeplant.