Technische Hochschule Ingolstadt

Modulhandbuch

Cybersicherheit (SPO WS 22/23)

Studien- und Prüfungsordnung: WS 22/23

Stand: 19.09.2022

Inhalt

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
Studienart & Abschlussgrad	Grundständiger B.Sc. in Vollzeit
Erstmaliges Startdatum	WS 2022/2023; jährlicher Start
Regelstudienzeit	7 Semester (210 ECTS, 125 SWS)
Lage des Praxissemesters	5. Semester
Studiendauer	
Studienort	THI Ingolstadt
Unterrichtssprache/n	überwiegend deutsch (ab 2. Semester in jedem Semester mindestens eine englische Lehrveranstaltung)
Kooperation	ESG Elektrosystemsystem- und Logistik-GmbH
Zulassungsvoraussetzung	Hochschulzugangsberechtigung
Kapazität	25 Studierende p.a.

Studiengangleiter:

Name: Prof. Dr.-Ing. Hans-Joachim Hof
E-Mail: hans-joachim.hof@thi.de (bevorzugte Kontaktmöglichkeit)
Tel.: +49 (0) 841 / 9348-2526 (bitte bevorzugte Kontaktmöglichkeit E-Mail verwenden)

2 Einführung

Als Teilgebiet der Informatik beschäftigt sich Cybersicherheit mit dem Schutz von Systemen und Informationen in allen 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 Studiengans 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
- Rahmenprüfungsordnung (RaPO)
- Allgemeine Prüfungsordnung (APO) der Technischen Hochschule Ingolstadt
- Immatrikulationssatzung der Technischen Hochschule Ingolstadt.

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

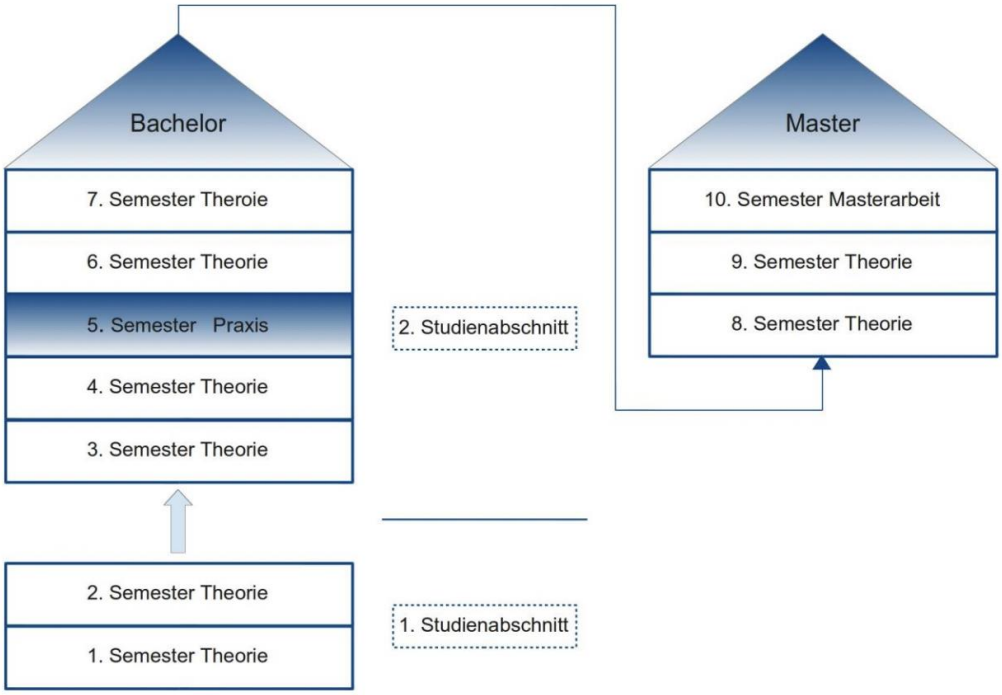
2.3 Zielgruppe

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.



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

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.

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, in der Rahmenprüfungsordnung (RaPo) und in der Allgemeinen Prüfungsordnung (APO) der Technischen Hochschule Ingolstadt.

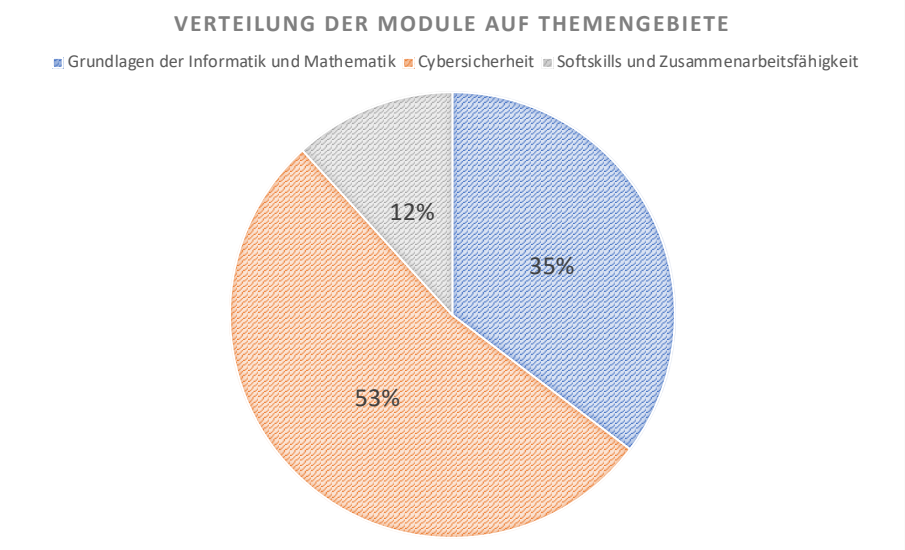
2.6 Konzeption und Fachbeirat

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 Sie 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

Lfd. Nr.	Modul	Art der Lehrveranstaltung	Prüfungsform
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
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

Lfd. Nr.	Modul	Art der Lehrveranstaltung	Prüfungsform
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
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, in

der Rahmenprüfungsordnung (RaPo), 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- & Selbstkopmetenz
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	++

Lfd. Nr.	Modul	Fachkompetenz Informatik/Mathematik	Fachkompetenz Cybersicherheit	Sozialkompetenz	Methoden- & Selbstkopmetenz
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
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

Lfd. Nr.	Modul	Fachkompetenz Informatik/Mathematik	Fachkompetenz Cybersicherheit	Sozialkompetenz	Methoden- & Selbstkopmetenz
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):	Hof, Hans-Joachim	
Dozent(in):	Hof, Hans-Joachim	
Leistungspunkte / SWS:	2 ECTS / 2 SWS	
Arbeitsaufwand:	Kontaktstunden: Selbststudium: Gesamtaufwand:	23 h 27 h 50 h
Lehrveranstaltungen des Moduls:	Einführungsprojekt	
Lehrformen des Moduls:	Prj - Projekt	
Prüfungsleistungen:	LN - ohne/mit Erfolg teilgenommen	
Verwendbarkeit für andere Studiengänge:	Keine	

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 spezifischer Themenstellung 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:

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.

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
Prüfungsleistungen:	2.1: schrP90 - schriftliche Prüfung, 90 Minuten 2.2: LN - ohne/mit Erfolg teilgenommen
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- 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.

Desweiteren wird dieses Image in den PC-Pools der Fakultät zur Verfügung gestellt.

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.

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 Wintersemester

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
Prüfungsleistungen:	3.1: schrP90 - schriftliche Prüfung, 90 Minuten 3.2: LN - ohne/mit Erfolg teilgenommen
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach Besuch des Moduls

- 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 Lagegrundlegende technische Konzepte der Ausführung von C++-Programmen zu verstehen, mit anderen Programmiersprachen zu vergleichen und zu bewerten.
- sind die Teilnehmer in der Lageeinfache Klassendiagramme zu verstehen und zu erstellen.
- sind die Teilnehmer in der Lageinformationstechnische 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:

- 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.

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
Prüfungsleistungen:	schrP90 - schriftliche Prüfung, 90 Minuten
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach Besuch des Moduls

- haben die Studierenden ein Grundverständniss davon, wie Algorithmen (Folgen von maschinell ausführbaren Rechenschritten) auf Rechnern (programmgesteuerten Informationsverarbeitungssystemen) ausgeführt werden.
- den Begriff des Algorithmus zu 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 sind die Studierenden in der Lage die Komplexität eines gegebenen Algorithmus abzuschätzen,
- zu verstehen, wie ein Algorithmus auf einem Rechner bearbeitet wird,
- sind die Studierenden in der Lage den Aufbau eines Universalrechners und seine Arbeitsweise zu beschreiben,
- sind die Studierenden in der Lageverschiedene fortgeschrittene Konzepte der Rechnerarchitektur einzuordnen.

Inhalt:

Algorithmen

- Algorithmenbegriff, Eigenschaften, Darstellungsformen
- Berechenbarkeit

- Turing-Berechenbarkeit
- LOOP-, WHILE-, GOTO-Berechenbarkeit
- Church-Turing-These
- Entscheidbarkeit, Halteproblem
- Komplexität
- O-Notation
- Komplexitätsklassen P und NP
- Rechnerarchitektur

Binäre Informationsdarstellung

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

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 - kurzgefasst*. Nachdruck der 5. Auflage. Heidelberg: Spektrum, Akad. Verl.. ISBN 978-3-8274-1824-1, 3-8274-1824-0
- PATTERSON, David A. und John L. HENNESSY, 2021. *Computer organization and design: the hardware/software interface*. S. Auflage. Amsterdam; Boston; Heidelberg ; London ; New York ; Oxford ; Paris ; San Diego ; San Francisco ; Singapore ; Sydney ; Tokyo: Morgan Kaufmann. ISBN 978-0-12-820109-1, 0128237163
- STALLINGS, William, 2016. *Computer organization and architecture: designing for performance*. 10. Auflage. Hoboken, NJ [u.a.]: Pearson Education.
- ZIEGENBALG, J, O ZIEGENBALG und B ZIEGENBALG, 2010. *Algorithmen von Hammurapi bis Gödel*. 3. Auflage. ISBN 9783817118649

Anmerkungen:

Bonuspunkteregelung: Für diese Vorlesung werden Bonuspunkte gemäß APO §8 Absatz (3) 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 Wintersemester

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
Prüfungsleistungen:	5.1: schrP90 - schriftliche Prüfung, 90 Minuten 5.2: LN - ohne/mit Erfolg teilgenommen
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

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-Digitalwandler)
- 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, Scheduling sowie Synchronisation
- Speicherverwaltung
- Dateisystem
- Ein-/Ausgabe, Gerätetreiber

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:

Das begleitende Praktikum umfasst 10 Aufgaben, die vorbereitet und im Labor vorgeführt werden müssen. Für das Bestehen ist der erfolgreiche Abschluss von 9 der 10 Aufgaben notwendig.

Bonuspunkteregelung: Für diese Vorlesung werden Bonuspunkte gemäß APO §8 Absatz (3) 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):	Hof, Hans-Joachim
Dozent(in):	Hof, Hans-Joachim
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
Prüfungsleistungen:	schrP90 - schriftliche Prüfung, 90 Minuten
Verwendbarkeit für andere Studiengänge:	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 zu ordnen

- 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)
Literatur:
ECKERT, Claudia, 2018. *IT-Sicherheit: Konzepte - Verfahren - Protokolle* [online]. München: De Gruyter Oldenburg 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, . *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. ISBN 3658362421
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):	Krüger, Max
Leistungspunkte / SWS:	6 ECTS / 5 SWS
Arbeitsaufwand:	Kontaktstunden: 58 h Selbststudium: 92 h Gesamtaufwand: 150 h
Lehrveranstaltungen des Moduls:	7.1: Mathematische Grundlagen 1 7.2: Übung zu Mathematische Grundlagen 1
Lehrformen des Moduls:	7.1: SU/Ü - seminaristischer Unterricht/Übung 7.2: Ü - Übung
Prüfungsleistungen:	7.1: schrP90 - schriftliche Prüfung, 90 Minuten 7.2: LN - ohne Leistungsnachweis
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

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 Gleichungssystemen 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 Wintersemester

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: Mathematische Grundlagen 2 8.2: Übung zu Mathematische Grundlagen 2
Lehrformen des Moduls:	8.1: SU/Ü - seminaristischer Unterricht/Übung 8.2: SU/Ü - seminaristischer Unterricht/Übung
Prüfungsleistungen:	8.1: schrP90 - schriftliche Prüfung, 90 Minuten 8.2: LN - ohne Leistungsnachweis
Verwendbarkeit für andere Studiengänge:	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:
- 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-Books. 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
Prüfungsleistungen:	schrP90 - schriftliche Prüfung, 90 Minuten
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

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 Wintersemester

Modulverantwortliche(r):	Apel, Sebastian
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 79 h Gesamtaufwand: 126 h
Lehrveranstaltungen des Moduls:	Software-Entwicklungsmethodik
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Prüfungsleistungen:	schrP90 - schriftliche Prüfung, 90 Minuten
Verwendbarkeit für andere Studiengänge:	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

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
Prüfungsleistungen:	13.1: schrP90 - schriftliche Prüfung, 90 Minuten 13.2: LN - ohne/mit Erfolg teilgenommen
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Keine

Angestrebte Lernergebnisse:

Nach Besuch des Moduls 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- & 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

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 und Datenbanksysteme 15.2: Praktikum Software-Design / SW-Architektur und Datenbanken
Lehrformen des Moduls:	15.1: SU/Ü - seminaristischer Unterricht/Übung 15.2: Pr - Praktikum
Prüfungsleistungen:	15.1: schrP90 - schriftliche Prüfung, 90 Minuten 15.2: LN - ohne/mit Erfolg teilgenommen
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

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 (Softwaredesign) 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-Books. 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