Qualifikationsziele
Bachelor Cyber Security

Fakultät Angewandte Informatik
der Technischen Hochschule Deggendorf

Verfasser: Prof. Dr. Martin Schramm, Studiengangskoordinator für den Bachelorstudiengang Cyber Security

Geschlechtsneutralität

Auf die Verwendung von Doppelformen oder anderen Kennzeichnungen weiblichen, männlichen und diversen Geschlechts wird weitgehend verzichtet, um die Lesbarkeit und Übersichtlichkeit zu wahren. Alle Bezeichnungen für die verschiedenen Gruppen von Hochschulangehörigen beziehen sich auf Angehörige aller Geschlechter der betreffenden Gruppen gleichermaßen.

Stand: 26.04.2021

Inhaltsverzeichnis

1 Ziele des Studiengangs

Der Bachelorstudiengang Cyber Security liefert die theoretischen und praktischen Grundlagen für Forschungs- und Entwicklungsaufgaben auf dem Gebiet der Cybersicherheit. Das Studium hat das Ziel, durch praxisorientierte Lehre auf wissenschaftlicher Grundlage, Grundkenntnisse und Fertigkeiten aus den wichtigsten Teilgebieten der Informatik zu vermitteln, welche in praktischen Anwendungen erforderlich sind. Durch eine umfassende Ausbildung sollen die Studierenden in die Lage versetzt werden, die wesentlichen Zusammenhänge im Themenkomplex Cybersicherheit zu erkennen. Studierende des Studiengangs sind in der Lage, komplexe Projekte der Cybersicherheit selbstständig und in Teams abzuwickeln, sowie agil auf rasch fortschreitende technische Entwicklungen reagieren zu können. Sie können die Auswirkungen der Vernetzung von Systemen auf unterschiedlichste Bereiche erkennen und die daraus resultierenden Chancen und Risiken bewerten. Die Absolventinnen und Absolventen sind in der Lage, über den bedarfsgerechten Einsatz von Mechanismen für die Absicherung (Härtung, Schutz) von IT-Systemen zu befinden. Sie kennen Methoden um Cyber-Vorfälle zu verhindern, zu erkennen und zu analysieren, können diese anwenden und für spezifische Einsatzbereiche adaptieren. Sie können selbstständig Risikobewertungen erstellen und IT-Systeme auditieren. Studierende vertiefen ihre Kenntnisse und spezialisieren sich durch Wahlpflichtmodule, die zur Flexibilisierung individueller Studienbiographien beitragen. Die Absolventinnen und Absolventen sind dazu qualifiziert, anwendungs- oder forschungsorientierte Aufgaben und Projekte fundiert und weitgehend selbstständig zu bearbeiten. Neben Fachwissen erwerben die Studierenden über Schlüsselqualifikationen soziale und methodische Kompetenz zur Förderung der Persönlichkeitsbildung, zur Arbeitsmethodik und Selbstorganisation, sowie zur Projektplanung und -abwicklung. Berufsmöglichkeiten bieten sich nicht nur in Wirtschafts- und Versorgungsunternehmen, sondern auch in den Verwaltungen des öffentlichen Dienstes sowie in der freien Praxis. Es wird auf eine breitgefächerte qualifizierte Ausbildung geachtet, die den Studierenden befähigt, in vielfältigen Berufsschwerpunkten zu arbeiten.

2 Lernergebnisse des Studiengangs

Das Studienprogramm soll die Studierenden dazu befähigen, typische Aufgaben eines Spezialisten für Cyber Security in der Industrie in den Bereichen Forschung und Entwicklung, und Projektdurchführung zu übernehmen. Ebenso ist die Beschäftigung im Öffentlichen Dienst, der Verwaltung, eine Tätigkeit als Berater bzw. unabhängiger

Gutachter, sowie der Weg in die Selbstständigkeit möglich. Das Programm, das insgesamt einen Umfang von 210 ECTS-Punkten besitzt, besteht aus sechs theoretischen (180 ECTS-Punkte) sowie einem Praxissemester (30 ECTS-Punkte) in Form eines Industriepraktikums. In den Theoriesemestern werden die mathematisch-naturwissenschaftlichen Grundlagen in den Modulen Mathematik 1, Mathematik 2 und Stochastik sowie informatische Grundlagen u.a. in den Modulen Grundlagen der Informatik, Betriebssysteme und Netzwerke, Programmierung 1, Programmierung 2, Algorithmen und Datenstrukturen, Internettechnologien und Datenbanken vermittelt. Kreditpunkte werden darüber hinaus in interdisziplinären Schlüsselqualifikationsmodulen (wie Medienkompetenz und Selbstorganisation, Betriebswirtschaft, Fachsprache, Technikethik und Nachhaltigkeit, Wissenschaftliches Arbeiten, Compliance, Datenschutz und IT-Recht, Team-Entwicklung und interkulturelle Kommunikation und Unternehmensgründung) erworben. Die Grundlagen der Cybersicherheit werden über Kernmodule (wie Kryptologie, Netzwerksicherheit, sichere Programmierung, Management und Auditierung von IT-Sicherheit, Penetration Testing und Digitale Forensik) vermittelt. Über Wahlpflichtmodule können sich die Studierenden weiter spezialisieren.

3 Studienziele und Qualifikationsziele

Die folgende Tabelle 1 ordnet den genannten Studienzielen im Bachelorstudiengang Cyber Security Lernergebnisse zu:

Tabelle 1: Lernergebnisse im Bachelorstudiengang Cyber Security	
1. Grundlagen aus den wichtigsten Teilgebieten der Mathematik und Informatik	Kenntnisse: Die Studierenden kennen grundlegende mathematische und informatische Begriffe und Methoden.
	Fertigkeiten: Auf Basis der Kenntnisse und Methoden können die Studierenden professionell Probleme analysieren und angepasste Lösungen entwickeln.
	Kompetenzen: Die wesentlichen Methoden der Mathematik und Informatik können angewendet werden.
2. Datenkompetenz, Analysekompetenz und Technologiekompetenz in den Kerngebieten der Cybersicherheit	Kenntnisse: Die Studierenden spezialisieren die allgemeinen Grundlagen in den Kerngebieten der Cybersicherheit.
	Fertigkeiten: Problemstellungen in den Kerngebieten der Cybersicherheit können analysiert und bewertet werden. Verfahren und Methoden aus den Kerngebieten der Cybersicherheit können bei neuen Problemstellungen angewandt werden.

	Kompetenzen: Problemstellungen zur Entwicklung neuartiger Cybersicherheits-Technologien können analysiert werden.
3. Cyber Security in der Anwendung	Kenntnisse: Die allgemeinen Grundlagen werden in verschiedenen Anwendungsbereichen spezialisiert.
	Fertigkeiten: Problemstellungen in den verschiedenen Anwendungsbereichen können analysiert und bewertet werden. Verfahren der Cybersicherheit können in den Anwendungsbereichen bei neuen Problemstellungen angewandt werden.
	Kompetenzen: Problemstellungen hins. Cybersicherheit bei der Entwicklung neuartiger Systeme in den Anwendungsbereichen können analysiert werden.
4. Überfachliche Kompetenz	Kenntnisse: Die wirtschaftlichen, rechtlichen und ethischen Rahmenbedingungen für die sichere Entwicklung, Ausgestaltung sowie Konfiguration und Nutzung von IKT-Systeme werden erkannt.
	Fertigkeiten: Studierende sind in der Lage, sich ein eigenes Meinungsbild zu schaffen und dieses verständlich zu präsentieren sowie eigene Ideen und Lösungen für Problemstellungen zu entwickeln und diese auch umzusetzen.
	Kompetenzen: Qualifizierte Einflussnahme auf die Entwicklung neuer IKT-Systeme unter Einhaltung der verschiedenen Rahmenbedingungen und Grundsätze (wie Security by Design, Privacy by Design). Bearbeitung von technischen Aufgabenstellungen im Team.

4 Lernergebnisse der Module / Modulziele

Die einzelnen Module, ihre Detailziele und die von den Absolventen zu erwerbenden Kompetenzen sind in den Modulhandbüchern für den Bachelorstudiengang Cyber Security beschrieben und auf der Webseite des Studiengangs veröffentlicht. Mit jedem Modul sollen die Studierenden ihr Kompetenzniveau erweitern. In der folgenden Tabelle wird der Zusammenhang zwischen den einzelnen Modulen und den im vorherigen Abschnitt beschriebenen Zielen im Bachelorstudiengang hergestellt:

Tabelle 2: Zielematrix der Module im Bachelorstudiengang Cyber Security

Module	Ziele											
	Kenntnisse				Fähigkeiten				Kompetenzen			
	Grundlagen	Technologiekompetenz	Anwendungen	Softskills	Grundlagen	Technologiekompetenz	Anwendungen	Softskills	Grundlagen	Technologiekompetenz	Anwendungen	Softskills
1. Semester												
Mathematik 1	xx				xx				x			
Programmierung 1	xx				xx				xx			
Grundlagen der Informatik	xx				xx				xx			
Betriebssysteme und Netzwerke	xx				xx				x			
Grundlagen der Informationssicherheit		xx				xx				x		
Schlüsselqualifikation 1				xx				xx				x
2. Semester												
Mathematik 2	xx				xx				x			
Programmierung 2	xx				xx				xx			
Algorithmen und Datenstrukturen	xx				xx				xx			
Internettechnologien	xx				xx				x			
Kryptologie 1		xx				xx				x		
Schlüsselqualifikation 2				xx				xx				x
3. Semester												
Datenbanken	xx				xx				x			
Stochastik	xx				xx				x			
Projektmanagement	x				xx				xx			
Sichere Programmierung			xx				xx				xx	
Netzwerksicherheit		xx				xx				xx		
Schlüsselqualifikation 3				xx				xx				x
4. Semester												
Software Engineering												
Wahlpflichtmodul Projekt			xx				xx				xx	
Kryptologie 2		xx				xx				xx		
Management von IT-Sicherheitsvorfällen			xx				xx				xx	
Distributed-Ledger-Technologien		xx				xx				xx		
Schlüsselqualifikation 4				xx				xx				x
6. Semester												
Penetration Testing			xx				xx				x	
Digitale Forensik			xx				xx				x	
Sicherheit interaktiver Systeme		x				xx				x		
Security Engineering		xx				xx				xx		
Wahlpflichtmodul 1			xx				xx				x	
Schlüsselqualifikation 5				xx				xx				x
7. Semester												
Auditierung von IT-Systemen			xx				xx				xx	
Wahlpflichtmodul 2			xx				xx				x	
Wahlpflichtmodul 3			xx				xx				x	

Legende: xx starker Bezug; x mittlerer Bezug