UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA
OBERÖSTERREICH

Campus Hagenberg

SIB

BSc

Sichere Informationssysteme

Vollzeit

Das Studium für den effektiven Schutz vor Cyberkriminalität, Hacking und Datendiebstahl

Im Unternehmensumfeld wie im privaten und öffentlichen Bereich gilt es, neue IT-Security-Herausforderungen in den Bereichen Cloud Security, IoT, Smart Technologies, Artifical Intelligence und Big Data zu meistern und sich den neuen Bedrohungen im Bereich Social Engineering und Hacking zu stellen. Dabei sind Netzwerke gegen unberechtigten Datenzugriff zu sichern, Attacken zu erkennen und forensisch zu analysieren, sicherheitskritische und ausfallssichere Systeme und Verfahren zu entwickeln sowie ein gesichertes Umfeld für die Kommunikation und den Schutz des Unternehmenswissens und von personenbezogenen Daten zu schaffen. Auf Basis der über 20jährigen Erfahrung im IT-Security-Ausbildungsbereich werden diese neuen Herausforderungen seit 2020 in einem neu gestalteten Studienplan besonders betont.

Karriere

Den Absolvent*innen eröffnet sich somit ein spannendes, vielfältiges und zukunftssicheres Betätigungsfeld als Security-Spezialist*innen in den Bereichen sichere Installation, Härtung und Betrieb von IT/Web/Internet-Systemen und Netzwerken, der Durchführung von Pentests und forensischen Analysen, der sicheren Softwareentwicklung sowie der Umsetzung von Informationssicherheits- und Notfallmanagementsystemen.

International

Das Berufspraktikum kann auch außerhalb Österreichs absolviert werden. Studierende waren zum Beispiel bei Siemens in Princeton (USA), dem Bundesamt für Sicherheit im Bereich Informationstechnologie in Bonn oder bei Firmen in Kanada, Dubai, China und Südafrika tätig. Partnerhochschulen gibt es unter anderem in Deutschland, Schweden und Japan.

Profil

Angaben in Prozent, basierend auf ECTS-Punkten

Akademischer Abschluss
→ Bachelor of Science in Engineering (BSc)

Studiendauer
→ 6 Semester (180 ECTS)

Zahl der Studienplätze je Studienjahr
→ 30

Zugangsvoraussetzungen
→ Hochschulreife
z. B. Matura/Abitur/Berufsreifeprüfung, einschlägige Studienberechtigungsprüfung/ FH OÖ-Studienbefähigungslehrgang

Bewerbung
→ online – Tipps & Termine auf fh-ooe.at/bewerbung

Aufnahmeverfahren
→ Bewerbungsgespräch

Anerkennung nachgewiesener Kenntnisse
→ individuell für Lehrveranstaltungen möglich

Praktikum
→ im 5. Semester im In- oder Ausland (mindestens 12 Wochen)

Kosten
→ € 363,36 pro Semester + ÖH-Beitrag für Studierende aus EU- und EWR-Staaten

fh-ooe.at/sib

Studienplan

Lehrveranstaltungen / ECTS / Semester	1	2	3	4	5	6
→ Wissenschaftliche Grundlagen + Technik						
Sichere Software						
Sichere Systemprogrammierung	8					
Sichere Anwendungsprogrammierung		6				
Scripting & Algorithmen		4				
Web			5			
Programmierpraktikum				3		
Sichere Infrastruktur						
Rechnerarchitektur	3					
Sichere Betriebssysteme	3					
Netzwerkanwendungen	3					
OS-, Netzwerk- und Kryptopraktikum		3		3		
Netzwerkgrundlagen		4				
Systemadministration (DevOps)			3			
Netzwerksicherheit			4			
Datenbanken			3			
Sichere verteilte Systeme				4		
Authentifizierungstechniken				2		
IoT Security						3
Software-Defined Everything						4
Mobile/Embedded OS						3
Hacking & PenTesting						
Malware und Underground Economy		2				
Reverse Engineering			4			
Penetration Testing				3		
Hacking-Praktikum						3
Incident Handling						
Systemplanung und IT-Servicemanagement			3			
Incident Analyse, IT-Forensik-Praktikum				3		
Informationssicherheits- & Notfallmanagement				3		
Industrial Security/Kritische Infrastrukturen						3
Kryptographie						
Anwendungen/Grundlagen der Kryptographie	3	5				
Fortgeschrittene Techniken der Kryptographie			3			
→ Fachübergreifende Qualifikationen						
Einführung in die Informationssicherheit	1					
Einführung Computeranwendungen	2					
Mathematik	4					
Projekt			1	3		3
Teamarbeit, Projektorganisation			2			
Organisation & Management						
Kommunikation und Organisation	3					
Betriebswirtschaftslehre		2				
Human Aspects of Information Security		2		2		
Sichere Geschäftsprozesse				1		
Informationsmanagment						3
Recht & Compliance						
IT-Security Rechtsgrundlagen		2				
Cybercrime-Recht						1
IT-Recht, aktuelles IT-Security-Recht			2			1
→ Wahlfächer, Berufspraktikum u. Seminar, Bachelorarbeit u. -prüfung						
Wahlfächer				2		5
Seminar wissenschaftliches Arbeiten				1		
Berufspraktikum und Seminar					22	
Bachelorarbeit, Seminar, Bachelorprüfung					8	1

Gut zu wissen

→ Das Security Forum in Hagenberg ist seit über 20 Jahren „die“ IKT-Sicherheitskonferenz, hier diskutieren internationale Expert*innen mit Besucher*innen und Studierenden.

ECTS: European Credit Transfer System.
Es sind jeweils 30 ECTS pro Semester (insgesamt 180 ECTS) zu absolvieren.

Themen

→ **Sichere Infrastruktur** beinflusst die Sicherheit von Anwendungen und Diensten wesentlich. Neben den notwendigen Grundlagen aus den Bereichen Hardware, Betriebssysteme, Computernetzwerke und Datenbanken werden Konzepte zur automatisierten, softwaregestützten Bereitstellung von Infrastruktur „on-premise“ aber auch in der Cloud vermittelt.

→ **Hacking & PenTesting:** Praktische Kompetenzen im Angreifen von Systemen, Software und Netzwerken sind wesentlich, um Angriffe besser zu verstehen und zu verhindern. Die erworbenen Fähigkeiten sind in vielen Berufsfeldern wie zum Beispiel Penetration Testing, IT-Forensik oder sicherer Softwareentwicklung von Bedeutung.

→ **Sichere Software:** Entscheidend für den Betrieb von zuverlässigen Systemen ist die Softwareentwicklung unter hohen Sicherheits- und Qualitätsaspekten auf allen Ebenen, vom Betriebssystem bis zur Applikation. Dafür werden die sichere System-, Anwendungs- und Webentwicklung, das korrekte Anwenden von Algorithmen sowie die Softwarequalitätssicherung sowohl theoretisch behandelt als auch praktisch in Übungen und Projekten angewendet.

→ **Kryptographie** ist ein Grundbaustein für sichere Systeme und sichere Kommunikation. Mit kryptographischen Verfahren können Daten vor unberechtigtem Zugriff geschützt, Veränderung an Daten erkannt und Urheber von Daten identifiziert werden. Das Wissen über moderne Verschlüsselungsalgorithmen und digitale Unterschriften ist Voraussetzung für das Entwickeln von sicheren Anwendungen.

→ **Recht & Compliance:** Auch das Einhalten relevanter Normen für IT-Systeme ist sicherzustellen. Im Rahmen von Recht und Compliance soll ein Überblick über die einschlägigen IT-Security Normen gegeben werden – von IT-Rechtsgrundlagen, über Grundzüge des Datenschutzrechts bis hin zu ganz spezifischen Vorgaben (z. B. kritische Infrastrukturen)

→ **Incident Handling:** Eine Voraussetzung für den sicheren Betrieb von IT-Systemen ist deren sorgfältige Planung und Dimensionierung sowie die Implementierung eines IT-Servicemanagements. Durch Informationssicherheits- und Notfallmanagement wird für die erforderlichen präventiven und reaktiven organisatorischen Maßnahmen zur Sicherstellung der IT-Security gesorgt, wobei der Schutz von kritischen Infrastrukturen und ICS-Systemen ein wichtiges Spezialgebiet darstellen. Incident Analyse & IT-Forensik sorgen bei Vorfällen für eine möglichst lückenlose Aufklärung.

→ **Organisation und Management:** Für eine umfassende und unternehmensweite IT-Security ist auch das sicherheitskonforme Verhalten von Mitarbeiter*innen von eminenter Bedeutung. Unternehmen haben immer häufiger mit folgenschweren Angriffen unter Ausnutzung der „menschlichen Schwachstelle“ zu kämpfen. Deshalb werden Themen wie Security Awareness, Social Engineering und sichere Geschäftsprozesse für Sicherheitsexpert*innen der Zukunft immer wichtiger. Diese werden im Studium eingehend vermittelt.

Kontakt

Department Sichere Informationssysteme

FH OÖ Fakultät für Informatik,
Kommunikation und Medien
Softwarepark 11, 4232 Hagenberg/Austria
+43 5 0804 22500 I sib@fh-hagenberg.at
fh-ooe.at/sib

12/23