© fotolia

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

SICHERE INFORMATIONSSYSTEME

BACHELORSTUDIUM, 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

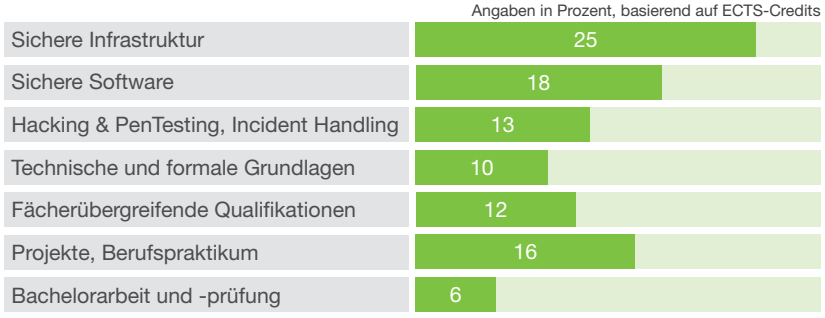
Den Absolvent*innen eröffnet sich somit ein spannendes, vielfältiges und zukunftssicheres Betätigungsfeld als Security Spezialist*innen in den Bereichen Sichere Softwareentwicklung, sichere Installation, Härtung und Betrieb von IT/Web/Internet-Systemen und Netzwerken, der Durchführung von Pentests und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



Kurzprofil

Akademischer Abschluss:
Bachelor of Science in Engineering (BSc)

Studiendauer:
6 Semester (180 ECTS)

Zahl der Studienplätze je Studienjahr: 30

Zugangsvoraussetzungen:
Hochschulreife (Matura, Reifeprüfung, Berufsreifeprüfung, Abitur), einschlägige Studienberechtigungsprüfung oder FH-Studienbefähigungslehrgang

Bewerbung:
online bis spätestens 30.6.
www.fh-ooe.at/bewerbung

Aufnahmeverfahren:
Potenzialtest und Bewerbungsgespräch

Anerkennung nachgewiesener Kenntnisse:
individuell für Lehrveranstaltungen möglich

Berufspraktikum:
im 5. Semester im In- oder Ausland (mindestens 12 Wochen)

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

www.fh-ooe.at/sib

Wussten Sie, dass ...

... Studierende von Sichere Informationssysteme das Security Forum am Campus Hagenberg organisieren, bei dem internationale Expert*innen zu aktuellen Themen der IKT-Sicherheit referieren und jährlich über 200 Besucher*innen erwartet werden?

Themen

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. Im Rahmen des Studiums werden dafür 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.

Sichere Infrastruktur: Die Sicherheit von Anwendungen und Diensten hängt wesentlich von der Sicherheit der darunterliegenden Infrastruktur ab. Neben den dafür 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: Kompetenzen im Angreifen von IT-Systemen sind wesentlich, um Angriffe besser verstehen und in weiterer Folge verhindern zu können. Dafür ist es wichtig, das Finden und Ausnutzen von Schwachstellen in Systemen, Software und Netzwerken, praktisch zu üben. Die erworbenen Fähigkeiten sind in vielen Berufsfeldern wie zum Beispiel Penetration Testing, IT-Forensik oder sicherer Softwareentwicklung von Bedeutung.

Kryptographie: 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: Zum korrekten Betrieb von IT-Systemen ist unter anderem auch das Einhalten relevanter Normen 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 bspw zum Schutz kritischer 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 d. IT-Security gesorgt, wobei der Schutz von kritischen Infrastrukturen und ICS-Systemen ein wichtiges Spezialgebiet darstellen. Sollte ein IT-Security Vorfall eintreten, so sorgen die Incident Analyse & IT-Forensik 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.

Studienplan

Lehrveranstaltungen	ECTS-Punkte pro Semester					
	1	2	3	4	5	6
Wissenschaftliche Grundlagen + Technik						
Sichere Software						
Sichere Systemprogrammierung	8					
Sichere Anwendungsprogrammierung		6				
Scripting & Algorithmen		4				
Web			5			
Softwareverifikation und -analyse			3			
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
Cloud Computing						2
Software-Defined Infrastructure						2
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				2		
Incident Analyse, IT-Forensik-Praktikum				3		
Informationssicherheits- & Notfallmanagement				3		
Industrial Security/Kritische Infrastrukturen						3
Kryptographie						
Anwendungen/Grundlagen der Kryptographie	3	5				
Fortgeschrittene Techniken d. Kryptographie			3			
Fachübergreifende Qualifikationen						
Einführung in die Informationssicherheit	1					
Einführung Computeranwendungen	2					
Mathematik	4					
Projekt/Softwareprojekt				4		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			1			2
Wahlfächer, Berufspraktikum u. Seminar, Bachelorarbeit u. -prüfung						
Wahlfächer						5
Seminar wissenschaftliches Arbeiten				1		
Berufspraktikum und Seminar					22	
Bachelorarbeit, Seminar, Bachelorprüfung					8	1

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

Weiterführende Masterstudien am Campus Hagenberg:

- Sichere Informationssysteme (Master)
- Information Security Management

Kontakt

Department Sichere Informationssysteme
FH OÖ Fakultät für Informatik, Kommunikation und Medien
Softwarepark 11, 4232 Hagenberg/Austria
Tel: +43 5 0804 22500
E-Mail: sib@fh-hagenberg.at, www.fh-ooe.at/sib