UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA
OBERÖSTERREICH

Campus Hagenberg

SIM

MSc

Vollzeit

Sichere Informationssysteme

Vertiefendes Know-how und Spezialisierung in Bereichen der Cybersecurity

Während Cybersecurity sich zunehmend zu einer Schlüsseltechnologie der modernen Kommunikationsgesellschaft entwickelt, bleibt die Verfügbarkeit von umfassend ausgebildeten Fachleuten mit Know-how im technischen, organisatorischen und juridischen Umfeld immer mehr hinter den aktuellen Erfordernissen zurück.

Das Masterstudium Sichere Informationssysteme vermittelt eben diese Kenntnisse in Kombination. Es eröffnet neben einer umfassenden Grundlagenausbildung die Möglichkeit zur individuellen Vertiefung und Spezialisierung in unterschiedlichen Bereichen der IT-Security und organisatorischen Informationssicherheit. Insbesondere werden dabei auch neue Technologien wie Quantum Computing und der Einsatz von Artificial Intelligence in Cybersecurity-Anwendungen vermittelt. Neben der professionellen, praxisbezogenen Ausbildung sind selbstständiges Arbeiten, wissenschaftliches Vorgehen und der Ausbau kommunikativer Fähigkeiten zentrale Anliegen.

Karriere

Absolvent*innen dieses Studiums eröffnen sich verschiedenste Tätigkeitsfelder, sowohl in der Entwicklung und Implementierung von Cybersecurity-Lösungen, im Auditierungs- und Zertifizierungsbereich, Projektmanagement als auch als selbstständige*r Berater*in sowie Systemplaner*in und -betreuer*in. Sie sind unter anderem verantwortlich für die Realisierung von Cybersecurity-Konzepten für vernetzte Informationssysteme (Cloud, Internet, Intranet), Security-Monitoring und -Managementsystemen (SIEM, SOC), für die Konzeption und Realisierung von Systemen zur sicheren Verarbeitung von sensiblen Daten (im Bereich kritischer Infrastrukturen, in Behörden & Ministerien, im Gesundheits- und Sicherheitswesen) oder auch für die Cybersecurity bei der Entwicklung von Kryptographie-, AI/KI- und Cloudsystemen. Ihre Expertise in Informationssicherheit und Sicherheitsmanagement ist in der Wirtschaft, in Unternehmensberatungen & Zertifizierungsstellen, bei CSIRTs sowie in öffentlichen Institutionen gefragt.

International

Der modulare Studienplan ermöglicht sowohl ein Auslandssemester als auch eine Forschungstätigkeit im Ausland im Rahmen der Masterarbeit. Partnerhochschulen gibt es unter anderem in Deutschland, Schweden und Japan.

Akademischer Abschluss
→ Master of Science in Engineering (MSc)

Studiendauer
→ 4 Semester (120 ECTS)

Zahl der Studienplätze je Studienjahr
→ 15

Zugangsvoraussetzungen
→ abgeschlossenes Bachelor- oder Diplomstudium (FH oder Universität) mit IT-relevanter Ausbildung im Umfang von mindestens 60 ECTS-Punkten

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

Aufnahmeverfahren
→ Bewerbungsgespräch

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

fh-ooe.at/sim

Studienplan

Lehrveranstaltungen	ECTS / Semester	1	2	3	4
→ Fachwissen					
IT- und IP-Recht, Ethik		7			
Cyber Defence, Digitale Forensik			7		
Digitale Identitäten, Sichere Infrastrukturen		5	10		
Security Engineering, Secure Systems Design		3	3	6	
Quantencomputing, Künstliche Intelligenz und Security		8			
Informationssicherheitsmanagement, Projektmanagement, -organisation und Teamführung		7			
→ Wahlpflichtfächer					
Wechselnde Inhalte				6	6
→ Wissenschaftliches Arbeiten					
Kolloquien, Scientific Writing			2		1
→ Projekte und Masterarbeit					
Projekt			8		
Vorprojekt zur Masterarbeit				18	
Masterarbeit, Masterprüfung					23

Themen

→ **Security Engineering, Secure Systems Design**
Die Entwicklung von sicheren IT-Systemen erfordert die Umsetzung von Securitymaßnahmen im Rahmen eines Secure System Lifecycles. Hierfür werden die wesentlichen Standards und Vorgehensweisen eines Secure Development Lifecycles sowie Werkzeuge und Techniken für dessen Umsetzung aus dem Bereich des risikobasierten Requirements Engineering benötigt. Der Lifecycle umfasst auch den Entwurf und die Implementierung von vertrauenswürdiger Software, Trusted Computing Plattformen sowie die Qualitätssicherung durch Reviews, Penetration Tests, Verifikation und Validierung.

→ **Digitale Identitäten**
Public-Key-Infrastrukturen (PKI) erlauben das Management von Schlüsseln, Rollen und Rechten. Kenntnisse über die Funktionsweise und den Betrieb der Komponenten einer PKI und der zugrundeliegenden kryptographischen Verfahren sind notwendig, um Dienste wie Authentifizierung, Verschlüsselung oder sichere Kommunikationssysteme entwickeln und betreiben zu können. Die manuelle und automatisierte Analyse und Bewertung solcher Verfahren sind wichtig für deren sichere Umsetzung.

→ **Quantencomputing, Künstliche Intelligenz und Security**
Die rasanten Entwicklungen der neuen Technolgien Quantum Computing und Artificial Intelligence stellen einerseits neue Bedrohungen im Cybersecuritybereich dar, erlauben aber auch die Entwicklung neuer Anwendungen im Cybersecurityumfeld. Um so wichtiger ist daher eine zukunftsorientierte fundierte Ausbildung in den Grundlagen und neuen Anwendungsfeldern wie Quantum Key Distribution oder AI/KI-Einsatz zur Analyse von securityrelevanten Daten.

→ **Sichere Infrastrukturen und Digitale Forensik**
Der hybride Betrieb von modernen IT-Systemen on premise und in der Cloud erfordert den Einsatz von skalierbaren und sicheren Netzwerkprotokollen und -technologien. Fundierte Kenntnisse über Softwaredefined Networks, Network Virtualization, Inter-Domain-Mechanismen und Security as a Service sind dabei essentiell. Digitale Forensik wird dabei zur Analyse von Cybersecurity-Incidents in verteilten, vernetzten Systemen benötigt.

→ **Informationssicherheitsmanagement und Cyber Defence**
Um in einem Unternehmen die Cybersecurity und Cyber Defence sicher zu stellen, sind Kenntnise der geltenden Sicherheitsanforderungen aus Gesetzen und branchenspezifischen Regelwerken, ein tiefes Verständnis der Cybersecurity Management-Aufgaben und der organisatorischen und technischen Rahmenbedingungen erforderlich. Aktuelle Informationssicherheits- und Risikomanagementmethoden zielgerichtet anzuwenden, um Sicherheitsorganisationen in Unternehmen aufzubauen und zu managen, stellen dabei die Grundlage dar.

→ **IT- und IP-Recht (Cyber Law)**
Zur Gewährleistung der Cybersecurity sind umfassende Kenntnisse der relevanten Rechtsgebiete erforderlich, vor allem im Bereich Cyberlaw, Internet- und Datenschutzrecht einerseits und zum Netz- und Informationssicherheitsrecht insbesonders im Bereich kritischer Infrastrukturanbieter (NIS) andererseits. Auch die speziellen regulatorischen Vorgaben für die Sicherstellung der technischen und organisatorischen Cybersecurity für Betreiber wesentlicher Dienste im NIS-Kontext sind dabei wesentlich.

→ **Ethik, Projektmanagement und Teamführungement**
Die Fähigkeit, Cybersecuritythemen erfolgreich kommunizieren und Teams effizient und motivierend führen zu können, ist von entscheidender Bedeutung. Die Konfrontation mit Themen- und Problemstellungen, die für eine Führungsrolle im Berufsleben wichtig sind, spielt dabei eine wesentliche Rolle. Auch die begleitende Persönlichkeitsentwicklung und die Reflexion von ethischen Aspekten relevanter Praxisfälle ist Bestandteil der Ausbildung.

Praxis und Forschung im Studium

In Projekten, Kolloquien und Wahlfächern vertiefen sich Studierende individuell in den vielfältigen Bereichen der Cybersecurity. Den Rahmen dazu bilden Projekt-Labs, in denen unter Leitung von FH-Professor*innen an Studierenden- und/oder Forschungsprojekten gearbeitet wird.

Zu den Forschungsschwerpunkten des Departments Sichere Informationssysteme zählen Incident-Analyse und -Response (Forensik), der Einsatz von quantensicheren kryptographischen Verfahren und Quantum Computing, der Einsatz von künstlicher Intelligenz (AI) im Analysebereich, Sicherheit im Bereich des Internet of Things (IoT) und Risikomanagement.

Gut zu wissen

→ Die mehr als 200 Absolvent*innen dieses Masterstudiums sind in über 20 Ländern und auf vier Kontinenten tätig.

ECTS: European Credit Transfer System
(= Anrechnungspunkte für Studienleistungen).
30 ECTS pro Semester (insg. 120 ECTS) sind zu absolvieren.

Kontakt

Department Sichere Informationssysteme

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

09/23