SICHERE INFORMATIONSSYSTEME

MASTERSTUDIUM, VOLLZEIT

Vertiefendes Know-how und Spezialisierung in Bereichen der IT- und Systemsicherheit

Während Sicherheit 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- und Systemsicherheit. 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 im Projektmanagement als auch in der Entwicklung oder als selbstständige*r Berater*in sowie Systemplaner*in und -betreuer*in.
Sie sind unter anderem verantwortlich für die Realisierung von Sicherheitskonzepten für vernetzte Informationssysteme (Internet, Intranet, Extranet), für die Konzeption und Realisierung von Informationssystemen zur Verarbeitung von sensiblen Daten (im Behördenumfeld, in Ministerien, Gesundheits- und Sicherheitswesen) oder auch für Entwicklungen im Kryptographie-, Biometrie- und Kommunikationssystembereich.

Ihre Expertise in Informationssicherheit und Sicherheitsmanagement ist in der Wirtschaft, in Unternehmensberatungen sowie in Körperschaften öffentlichen Rechts 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. Absolvent*innen sind in über 20 Ländern und auf vier Kontinenten tätig.

Wussten Sie, dass ...

... Absolvent*innen dieses Masterstudiums in über 20 Ländern und auf vier Kontinenten tätig sind?

Kurzprofil

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 bis spätestens 30.6.
www.fh-ooe.at/bewerbung

Aufnahmeverfahren:
Bewerbungsgespräch

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

www.fh-ooe.at/sim

Sicherheitsrisiken zu beherrschen und sensible Informationen und IT-Systeme wirksam zu schützen wird nicht nur immer wichtiger, sondern auch technisch und organisatorisch immer anspruchsvoller. Wir bilden in unserem Master für diese Aufgaben kompetente Expert*innen aus.

FH-Prof. DI Dr. Jürgen Fuß, *Studiengangskoordinator*

Themen

Informationsmanagement

Die Aufgabenstellung, in einem Unternehmen für die Informationssicherheit verantwortlich zu sein, erfordert sowohl die Kenntnis der geltenden Sicherheitsanforderungen aus Gesetzen und branchenspezifischen Regelwerken als auch ein tiefes Verständnis für die eigene Rolle und die organisatorischen Rahmenbedingungen. Studierende erwerben die Fähigkeit, aktuelle Risikomanagementmethoden zielgerichtet anzuwenden sowie mit Hilfe von praxisorientierten Übungen, Case Studies, Gastvorträgen erfahrener CISOs und Exkursionen das grundlegende Wissen, Sicherheitsorganisationen in Unternehmen aufzubauen und zu managen.

Digitale Identitäten

Public-Key-Infrastrukturen (PKI) erlauben das Management von Schlüsseln, Rollen und Rechten. Kenntnis über Funktionsweise und Betrieb der verschiedenen Komponenten einer PKI ist notwendig, um PKI-basierte Dienste wie Authentifizierung und Verschlüsselung zur Verfügung stellen zu können. Starke Authentifizierungsverfahren auf Basis kryptographischer Algorithmen stellen die Grundlage für sichere Kommunikation und für Zugriffskontrolle dar. Die manuelle und automatisierte Analyse und Bewertung solcher Verfahren sind wichtig für deren sichere Umsetzung.

Secure Software Engineering

Die Entwicklung von sicheren Softwaresystemen umfasst sowohl die paradigmenabhängige Planung als auch die Umsetzung eines Secure Software Development Lifecycles. Hierfür werden die wesentlichen Standards und Vorgehensweisen eines Secure Software Development Lifecycles sowie Werkzeuge und Techniken für dessen Umsetzung aus dem Bereich des risikobasierten Requirements Engineering vermittelt. Das beinhaltet auch den Entwurf und die Implementierung von vertrauenswürdigen Softwarearchitekturen sowie deren Qualitätssicherung über den gesamten Lifecycle durch Reviews, Code Review, Testen und die Verifikation und Validierung.

Netzwerke und Netzwerksicherheit

Die Funktionsweise und die Sicherheit von Diensten, die für das Internet in seiner Gesamtheit von Bedeutung sind, wie beispielsweise DNS, Routing und Content Delivery, stehen im Fokus des Schwerpunkts Netzwerke und Netzwerksicherheit, der sich darüber hinaus noch mit Konzepten und Tools zur Erkennung von Angriffen in Netzwerken beschäftigt.

Recht

Zur Gewährleistung von sicheren Informationssystemen wird ein umfassender Einblick in die davon betroffenen Rechtsgebiete gegeben - dabei vor allem zum Datenschutzrecht einerseits und zum Netz- und Informationssicherheitsrecht insb. im Bereich kritischer Infrastrukturanbieter andererseits. Zudem werden bestehende Schutzrechte mit IT- und Online-Bezug dargestellt und ein Überblick zu den Grundlagen des Urheberrechts bzw. Patentrechts gegeben.

Ethik-Teamführung-Kommunikation

Die Fähigkeit, Informationssicherheitsthemen erfolgreich kommunizieren und Teams effizient und motivierend führen zu können, ist für Sicherheitsexpert*innen von entscheidender Bedeutung. Im Rahmen dieses Moduls werden die Studierenden mit Themen- und Problemstellungen konfrontiert, die für die spätere Übernahme einer Führungsrolle im Berufsleben wesentlich sind. Der Bogen spannt sich dabei von praktischen Übungen zum Kommunikationsverhalten in Führungssituationen über die begleitende Persönlichkeitsentwicklung bis hin zur Reflexion der ethischen Aspekte von relevanten Praxisfällen.

Praxis und Forschung

In Projekten, Projektseminaren und -kolloquien vertiefen sich Studierende individuell in einem Bereich der Informationssicherheit. Den Rahmen dazu bilden Labs, in denen unter Leitung von FH-Professor*innen an Studierenden- und/oder Forschungsprojekten gearbeitet wird.

Zu den Forschungsschwerpunkten des Departments Sichere Informationssysteme zählen der Schutz kritischer Infrastrukturen, Incident-Analyse und -Response (Forensik), die Verbesserung kryptographischer Verfahren, sichere Systemimplementierung, das Erkennen von Schadsoftware und Bedrohungen über das Internet, Risikomanagement sowie der Aufbau sicherer Unternehmensorganisationen.

Studienplan

Lehrveranstaltungen	ECTS-Punkte pro Semester			
	1	2	3	4
Grundlagen				
Grundlagen wissenschaftlichen Arbeitens	5			
Fachwissen				
Netzwerke und Netzwerksicherheit	3	3		
Informationsmanagement	3	3		
Digitale Identitäten	3	3		
Secure Software Engineering	3	3		
Ethik – Teamführung – Kommunikation	2	2	2	
Recht und Datenschutz	3			
Wahlpflichtfächer				
Wechselnde Inhalte		3	6	
Seminare				
Aktuelle Sicherheitsthemen		2	2	2
Projekte und Masterarbeit				
Orientierungsprojekt	8			
Projekt		11		
Vorprojekt			20	
Masterarbeit				28

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

Kontakt

Studiengangsleiter: FH-Prof. DI Robert Kolmhofer
Studiengangskoordinator: FH-Prof. DI Dr. Jürgen Fuß
Studiengangsadministration: Yvonne Füreder, Bakk. techn.
FH OÖ Fakultät für Informatik, Kommunikation und Medien
Softwarepark 11, 4232 Hagenberg/Austria
Tel: +43 5 0804 22500
E-Mail: sim@fh-hagenberg.at, www.fh-ooe.at/sim