

# IT AND MOBILE SECURITY

Mit diesem Master treffen Sie den Nerv der Zeit: Die Sicherheit von sensiblen Daten, Netzwerken und Systemen ist wichtiger als je zuvor. Cyberangriffe auf Unternehmen und Privatpersonen sind zur Normalität geworden. Hier sind hoch qualifizierte Spezialist:innen für die Entwicklung und Implementierung sicherer Software stark gefragt. Finden Sie mit uns neue Wege zu mehr IT-Sicherheit für digitale Lösungen.

## IT Security

Sie beschäftigen sich mit Firewall-Technologien, sicheren Netzwerkarchitekturen oder forensischen Untersuchungen. Außerdem stehen die Schwachstellenanalyse in Computersystemen und die Identifikation von Schadsoftware im Fokus. Sie lernen kreative Methoden von Hacker:innen kennen, um effektive Schutzmechanismen im Netzwerk, in Serversystemen und in mobilen Anwendungen zu implementieren.

## Software Security

Sie lernen Methoden der sicheren Softwarearchitektur und des Softwaredesigns kennen. Damit sind Sie in der Lage, sichere Software zu entwickeln und zu implementieren. Sie vertiefen sich nicht nur in das Thema Kryptographie, sondern Sie beschäftigen sich auch mit der konkreten Umsetzung von Software auf verschiedenen Betriebssystemen sowohl im Web als auch im Server-, Cloud- und mobilen Bereich. Künstliche Intelligenz und Machine Learning sind ein fester Bestandteil in der Analyse von Cyberangriffen und der Reaktion auf unbekannte Bedrohungen.

## Security Management

Neben den Spezial-Skills im technischen Bereich beschäftigen Sie sich auch mit Standards aus der IT-Informationssicherheit, dem Risikomanagement sowie mit Methoden des IT-Projekt- und Change-Managements. Die Behandlung von rechtlichen, sozialen und ethischen Aspekten runden das Thema ab.

## Projektarbeit. Masterarbeit

Ihr Wissen auf dem Gebiet der IT-Sicherheit vertiefen Sie außerdem in der Projekt- und Masterarbeit.

## FACTS



Master of Science in Engineering (MSc)



Berufsbegleitend



4 Semester / 120 ECTS



FH JOANNEUM Kapfenberg



Unterrichtssprache: Deutsch / Englisch

- 20 Studienplätze pro Jahr
- Studiengangsleiterin: **FH-Prof. Mag. Dr. Sonja Gögele, MBA MSc**
- Studiengebühren: keine für Studierende aus der EU, dem EWR und der Schweiz
- Alle Infos zu Terminen, Voraussetzungen, Bewerbung und Aufnahmeverfahren finden Sie online.
- [www.fh-joanneum.at/ims](http://www.fh-joanneum.at/ims)

## Wussten Sie, ...

... dass jedes Jahr Studierende, wie auch Absolvent:innen dieses Studienganges bei der Austria Cyber Security Challenge im Finale stehen? Durch so eine Teilnahme können unzählige Kontakte geknüpft und Erfahrungen gesammelt werden.



## Organisation

Durch den hohen E-Learning-Anteil lässt sich das Studium gut mit Beruf und Familie vereinbaren. Eine Anwesenheit vor Ort ist nur an zwei Wochenenden pro Monat, Freitag und Samstag, notwendig. Zusätzlich gibt es zwei Präsenzblöcke (DO bis SA, 08:45 bis 16:30) je Semester.

**Unterrichtszeiten:** DO: 18:00 bis 21:15 online | FR: 14:00 bis 21:15 online/präsent | SA: 08:45 bis 16:30 online/präsent.

## Berufsfelder

Unsere Absolvent:innen sind überall dort tätig, wo sensible Daten verarbeitet werden, etwa in IKT-Dienstleistungsunternehmen, bei Providern, in Unternehmen mit Fokus auf Datenbanken, in Systemhäusern, Consulting-Firmen und im Bereich Datensicherheit. Neben der Verfolgung und Aufklärung von Cyberkriminalität, gründen viele auch eigene Unternehmen im Bereich der IT-Security-Dienstleistungen. Dieses Studium bereitet nicht nur auf eine Karriere in der IT-Sicherheit vor, sondern schafft auch die Voraussetzungen für ein Doktoratsstudium.

*„Die stetig wachsende Vernetzung birgt ein erhöhtes Risiko von Cyberangriffen, Datenlecks und digitalen Bedrohungen. Eine robuste IT-Security-Ausbildung ist notwendig, um persönliche Daten, Unternehmensgeheimnisse und kritische Infrastrukturen zu schützen. Durch die Gewährleistung der IT-Sicherheit tragen wir nicht nur dazu bei, Vertrauen in digitale Dienste aufrechtzuerhalten, sondern schaffen auch eine sichere Grundlage für Innovation und Fortschritt. Den digitalen Raum abzusichern, bedeutet die Privatsphäre zu wahren, finanzielle Verluste zu minimieren und die Integrität unserer vernetzten Gesellschaft zu bewahren.“*

FH-Prof. Dr. Klaus Gebeshuber, Lehrender

CURRICULUM: 120 ECTS (30 ECTS pro Semester)

1. Semester	LV-Typ	SWS	ECTS
Software Security	ILV	3	3,5
Security Fundamentals	SE	1	3,5
Cryptography	VO	4	5
Basic Network Security	ILV	4	5
Secure Android Development	ILV	4	4
IT-Project-and Change Management	SE	2	4
Cloud Computing	ILV	2	3
Operating Systems	ILV	2	2
		<b>22</b>	<b>30</b>

3. Semester	LV-Typ	SWS	ECTS
Secure Web Applications	UE	3	5
Project Work	SE	9	10
Scientific Research	SE	2	5
Secure Systems	ILV	2	3
Cybercrime	VO	2	2
Advanced System Exploitation	UE	2	3
Operating System Security	ILV	2	2
		<b>22</b>	<b>30</b>

2. Semester	LV-Typ	SWS	ECTS
Mobile Network Security	ILV	3	5
Secure Software Design	ILV	3	5
Ethical Hacking	ILV	3	5
Database Security	SE	2	2
Machine Learning and AI for Security	ILV	2	2
Privacy and Data Protection	VO	2	3
Applied Cryptography	ILV	3	3
Secure IOS Development	UE	3	5
		<b>21</b>	<b>30</b>

4. Semester	LV-Typ	SWS	ECTS
Master Thesis	MA	0,5	14
Workshop on Master Thesis	SE	3	2,5
Ethics and Technology Assessment	SE	2	2,5
Examination on Master Thesis	FA	0	1
Security Management	SE	3	5
Secure Server Environments	SE	2	3
Embedded Security Assessment	ILV	2	2
		<b>12,5</b>	<b>30</b>

FA = Abschlussprüfung, ILV = Integrierte Lehrveranstaltung, MA = Master Thesis, SE = Seminar, UE = Übung, VO = Vorlesung, SWS = Semesterwochenstunden, ECTS = Europäisches System zur Übertragung und Akkumulierung von Studienleistungen