

Information Security

Masterstudium

■ Vollzeit

www.fhstp.ac.at



studies/graduate/information security

/fh///
st.pölten

Information Security

Der Masterstudiengang Information Security vermittelt eine Kombination aus technischen Kenntnissen und Management Know-how, die in keinem anderen Bildungszweig in dieser Tiefe angeboten wird. Information Security bildet ExpertInnen aus, die den stetig zunehmenden Anforderungen im IT-Bereich gewachsen sind. Ihre praxisorientierte Ausbildung bereitet Sie darauf vor, die Sicherheit von Gesamtsystemen besser zu garantieren und Informationssicherheit im Unternehmen zu verankern.



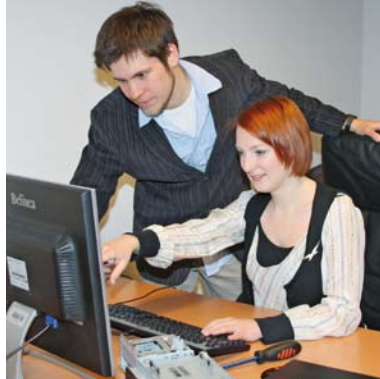
„Neben soliden fachlichen Kenntnissen verfügen die AbsolventInnen über die nötige Managementkompetenz, um berufliche Herausforderungen zu meistern.“

FH-Prof. DI Johann Haag,
Studiengangsleiter

IT Sicherheit. Ein Feld, das sich laufend verändert. Ein rasanter Wandel folgt dem nächsten. Genügte vor wenigen Jahren einfache Sicherheitsmechanismen an den Unternehmensgrenzen, stellen sich heute neue, komplexere Anforderungen an IT Gesamtsysteme. Die Gründe dafür sind schnell genannt: Flexible Unternehmensorganisationen, mobile Endgeräte und firmenübergreifende Projektkulturen stellen die IT Sicherheit vor neue Herausforderungen. Unternehmen verlangen nach ExpertInnen, die den heutigen wie künftigen IT Sicherheitsanforderungen gewachsen sind.

Veränderungen sicher meistern. Das Berufsfeld der Information Security AbsolventInnen hat sich entwickelt – und die Aufgabenverteilung neu sortiert: Zu den klassischen Aufgaben der AdministratorInnen/SystemintegratorInnen gesellen sich Schwerpunkte im Technik- und Sicherheitsmanagementbereich und erstrecken sich hin zum „Solution Architect“. Also jenen ExpertInnen, die sich der Gesamtbetrachtung und Analyse der verwendeten IT Systeme in Unternehmen annehmen. Gleichzeitig wissen diese ExpertInnen über die gesetzlichen und wirtschaftlichen Rahmenbedingungen Bescheid.

Unternehmenskritische Informationen zuverlässig schützen.



Fachlich und praktisch kompetent. Informationssicherheit ist nicht nur eine Frage der Technik, sondern hängt stark von den organisatorischen und personellen Rahmenbedingungen ab. Das Masterstudium vermittelt Ihnen eine Kombination aus technischen Kenntnissen und Management Know-how. Information Security bereitet Sie professionell auf Tätigkeiten vor, die ein Chief Security Officer erfüllen muss. AbsolventInnen haben neben fachlichen und praktischen Kenntnissen auch die notwendige Managementkompetenz, die Sie für Ihre berufliche Karriere brauchen. Fächerübergreifende Problemstellungen, Forschungsseminare, Projekte und die wissenschaftliche Abschlussarbeit (Diplomarbeit) bereiten darauf vor.

In Vorbereitung auf das wissenschaftliche Arbeiten können Sie sich an der so genannten „Forschungswerkstatt“ beteiligen. Dort arbeiten Sie an aktuell genehmigten Projekten mit und vertiefen Ihre Fachkenntnisse.

Ausbildungsinhalte

Der Masterstudiengang Information Security ist ein konsekutiver Studiengang, der auf dem Bachelorstudiengang IT Security aufbaut. Die Ausbildung besteht aus fünf Schwerpunkten:

- IT Infrastruktur (Betriebssicherheit und Netzwerksicherheit)
- Sicherheitstechnologien (Kryptografie und Biometrie)
- Software Engineering
- Sicherheitsmanagement (IT Compliance und Recht)
- Wirtschaft

Im Bereich **IT Infrastruktur** werden die Kompetenzen für einen sicheren und zuverlässigen Betrieb des Kommunikationsflusses sichergestellt. Dazu gehört das notwendige Wissen für ein sicheres Design solcher Gesamtsysteme (Daten- und Sprachkommunikationsnetze in Verbindung mit Sicherheitskomponenten), aber auch Wissen, um Sicherheitslücken zu erkennen bzw. zu finden.

Der Schwerpunkt **Sicherheitstechnologien** vertieft die Themengebiete Kryptografie und BenutzerInnenauthentifizierung. In der Kryptografie werden vor allem Implementierungen und Gesamtsysteme in Unternehmen betrachtet, in der BenutzerInnenauthentifizierung moderne biometrische Verfahren vorgestellt.

Software Engineering betrachtet die Sicherheit jener Applikationen, die im Internet oder im täglichen Geschäftsprozess verwendet werden. Dazu gehört der gesamte Softwareentwicklungsprozess inklusive Sicherheitszertifizierung genauso wie die entsprechenden Testverfahren bei der Übernahme von Software.

Der Bereich **Sicherheitsmanagement** hat das Ziel, Sicherheit messbar und überprüfbar zu machen.

Dadurch können laufend Verbesserungen erarbeitet bzw. Schwachstellen erkannt werden. Das erfordert umfassende Kenntnisse der gesetzlichen Regelungen und die Fähigkeit, im IT Bereich das zu tun, was dem Gesamtunternehmen am meisten nützt. (Compliance).

Der Bereich **Wirtschaft** vermittelt das notwendige Grundwissen, um Werteflüsse und Alternativen wertmäßig darstellen zu können. Bei der Einführung von Sicherheitspolicies sind die AbsolventInnen des Masterstudiengangs kompetente GesprächspartnerInnen für Finanzverantwortliche. Sie haben sich im Laufe des Studiums Wissen angeeignet, um Projekte und Prozesse professionell und wirtschaftlich zu leiten. Gleichzeitig verfügen Sie über genügend Grundwissen was Managementtechniken und Businesspläne anbelangt.

Projekte

Hacking Lab: StudentInnen entwickelten ein Konzept für den einfachen und flexiblen Betrieb eines virtuellen Computer Labors, dem „Secure Hacking Lab“.

Mit diesem Hacking Lab ist es möglich, individuelle aktuelle Hacking-Aufgabenstellungen für Unterrichtszwecke anzubieten. Dabei wird verhindert, dass „gegenseitige“ Hack-Übergriffe zwischen den TeilnehmerInnen möglich sind. Durch diese Lösung mittels einer „Private Cloud“ ergibt sich ein geringer administrativer Aufwand mit hoher Flexibilität für den/die Betreiber.

Biometrische Gesichtserkennung – Projekt FaceMoc: Zeig mir dein Gesicht und ich sage dir, wer du bist! In der Informationstechnologie bedeutet Biometrie das Erkennen von BenutzerInnen aufgrund ihrer persönlichen Eigenschaften. Mit Hilfe von biometrischen Verfahren werden physische und verhal-

tenstypische Merkmale erfasst und können direkt auf einem Chip gespeichert werden. Der bekannteste biometrische Mustervergleich ist der Fingerabdruck. Die biometrische Gesichtserkennung am Chip jedoch stellt ForscherInnen noch vor viele Rätsel. Mit dem Projekt FaceMoc trägt u. a. der Studiengang IT Security zur Lösung dieser offenen Forschungsfragen bei.

Business Continuity Management:

Um bei Vorfällen oder im Katastrophenfall die Abwicklung der Unternehmensgeschäfte fortzuführen (Business Continuity), müssen Analysen und Planungen vorgenommen werden. Gemeinsam mit einer Partnerfirma erstellten die Studierenden ein Business Continuity Readiness Modell inkl. einer Szenario-Datenbank, um Planungs- und Testaktivitäten im Bereich Business Continuity zu verbessern.

Automatische Malware-Analyse: Schadensbegrenzung auf hohem Niveau. Bei diesem Projekt wurden effiziente Verfahren entwickelt, um rasch verdächtige Code-Samples für eine dynamische Code Analyse zu bewerten. Der Prototyp stellte die Aktivitäten des Codes dar. Diese werden bewertet, woraus sich erste Einschätzungen der Gefährlichkeit des Samples ablesen lassen.

Kooperationen

Was wäre die Theorie ohne die Praxis? Für Sie als künftige IT Security ExpertInnen ist es von Anfang an wichtig, Kontakte zu Unternehmen und Wirtschaft zu knüpfen. Denn nur so können Sie Ihr theoretisches Wissen in die Praxis umsetzen, an Unternehmensprojekten mitarbeiten und künftige ArbeitgeberInnen von Ihrem Können überzeugen. Der Studiengang konnte zahlreiche österreichische und internationale namhafte Unternehmen für die Mitarbeit gewinnen.



Studiengang im Überblick

Abschluss: Diplom-Ingenieur/Diplom-Ingenieurin (DI)
Studiendauer: 4 Semester
Organisationsform: Vollzeitstudium, Masterstudium
Zahl der Studienplätze/Jahr: 20

Auslandssemester an einer internationalen Partnerhochschule ist möglich und erwünscht

Chancen und Berufsfelder

Angesichts der ständigen Entwicklung und Ausweitung der Informations- und Kommunikationstechnologie erweitern sich die Tätigkeitsfelder für Information Security ExpertInnen kontinuierlich.

Als AbsolventInnen des Masterstudiengangs Information Security sind Sie in der Lage, sichere Gesamtsysteme zu entwickeln bzw. vorhandene Systeme auf Schwachstellen zu untersuchen. Sie haben das Wissen, um geeignete Gegenmaßnahmen sowohl technischer als auch organisatorischer Natur zu entwerfen.

Es ergeben sich dadurch beispielhaft folgende Berufsfelder für AbsolventInnen:

- Sicherheitsbeauftragte/r (Chief Information-Security-Officer)
- Compliance Officer, RisikomanagerIn
- IT-Governance ExpertIn
- Datenschutzbeauftragte/r
- AuditorIn
- IT Security Solution Engineer/Architect
- Security-Consultant
- IT Infrastructure Engineer
- Security Quality Assurance ManagerIn
- Software Architect
- IT-Solution Architect

Vielseitige, attraktive Berufsperspektiven in anspruchsvollen Tätigkeitsbereichen in Industrie, Handel, Versicherungen, Dienstleistungen, Unternehmensberatung, Öffentlicher Verwaltung und nicht zuletzt in der Forschung erwarten Sie.

Beispiele aus dem Berufsleben

Der Sicherheitsbeauftragte **Chief Security Officer (CSO)** ist der/die Konzernverantwortliche für den Bereich Sicherheit. In den Tätigkeitsbereich fallen IT- und Informationssicherheit, organisatorische und physische Sicherheit aber auch elektronische und mechanische Sicherheitseinrichtungen. Der CSO ist direkt verantwortlich für Durchführung, Einhaltung und Entwicklung von sicherheitsrelevanten Themen.

Security Policies sind notwendig, um Sicherheit messbar zu machen. Der/die **AuditorIn** überprüft die Einhaltung dieser Regeln und gibt entsprechende Empfehlungen an die Unternehmensleitung weiter.

Der **IT Security Solution Engineer/Architect** entwickelt nach Kundenanforderungen sichere Gesamtsysteme. Dazu gehört eine entsprechende sichere Authentifizierung (ev. mit Kartensystemen), eine Absicherung an den Unternehmensgrenzen (mit Firewallsystemen), eine entsprechende Sicherheit am Client sowie ein sicherer und zuverlässiger Betrieb entsprechender Mail- und Webservices.

Safety & Security ManagerInnen entwickeln konzernweit gültige Security-Policies und stellen ihre Umsetzung im täglichen Betrieb sicher. Sie designen Basel II und Sox konforme Backup und Recovery Vorgaben/Strategien und konzipieren mit den Fachabteilungen maßgeschneiderte Umsetzungspläne.

Zugangsvoraussetzungen

Die Qualifikation zum Masterstudium Information Security erbringen Sie durch ein abgeschlossenes Bachelorstudium mit IT-Elementen von mindestens 60 ECTS. Davon müssen mindestens 12 ECTS im Bereich Security oder Software-Engineering enthalten sein.

Bewerbung / Aufnahmeverfahren

Für das Auswahlverfahren werden ausschließlich leistungsbezogene Kriterien angewandt.

Es gliedert sich in zwei Stufen:

- Bewerbung inkl. Motivationsschreiben, Zeugnissen und Lebenslauf
- Aufnahmegespräch

Beratungs- und Aufnahmegespräche finden im Sommersemester statt.

Nähere Informationen finden Sie unter www.fhstp.ac.at bzw. erhalten Sie in unserem Sekretariat unter Tel. +43/2742/313 228 - 632