

# IT Security

Bachelorstudium

■ Vollzeit

**/fh///**  
st.pölten

studies/undergraduate/it security



[www.fhstp.ac.at](http://www.fhstp.ac.at)

# IT Security

**Ihr Studium. Eine sichere Sache.** Das Bachelorstudium IT Security vermittelt Ihnen eine integrale, ganzheitliche Sicht der Security von IT-Infrastruktur. Das Besondere – und in Österreich Einzigartige – daran ist die Kombination aus Technik- und Managementwissen. Als künftige IT Security ExpertInnen bereitet Sie das Studium auf den IT Security Alltag in Unternehmen vor. Organisatorische und Managementaufgaben inklusive.



„Die Kombination aus Technik- und Managementwissen ist in Österreich einzigartig und bildet die Grundlage für die zukünftigen SecurityexpertInnen im Unternehmen.“

FH-Prof. DI Johann Haag,  
Studiengangsleiter

**IT Security. Ein Überblick.** In modernen Businessbereichen spielen flexible Endgeräte, unabhängige Arbeitsmodelle eine immer größere Rolle. IT-BenutzerInnen werden mobiler und unabhängiger. Laptops, PDA's und ähnliche Geräte erleichtern hierbei die Vernetzung und Übertragung von Daten über Unternehmensgrenzen hinweg. Was für den einen Arbeitserleichterung bedeutet, verlangt bei anderen nach höherem Sicherheitschutz. Computerviren, Hacker, Datenverluste, Webattacks usw. stellen eine enorme Bedrohung für die IT-Infrastruktur eines Unternehmens dar. Auch die immer stärkere Medienpräsenz von Informationssicherheitsgefahren, die ihren Höhepunkt mit Stuxnet und den Veröffentlichungen auf WikiLeaks gefunden hat, zeigt den wachsenden Markt für InformationssicherheitsspezialistInnen.

**Sie sind gefragt.** Der Ruf nach gut ausgebildeten ExpertInnen auf akademischem Niveau mit Fokus IT Sicherheit wird immer lauter. Als AbsolventIn des Bachelorstudiengangs IT Security beherrschen Sie die technischen Grundlagen für einen sicheren IT-Betrieb. Sie kümmern sich gleichzeitig um die laufenden organisatorischen Anforderungen und Managementaufgaben, um die EDV-Infrastruktur sicher zu betreiben.

# IT-Infrastruktur sichern und managen.

## Ausbildungsinhalte

Die Ausbildung besteht aus vier Schwerpunkten:

- IT-Betrieb
- Netzwerktechnik
- Sicherheitstechnologien
- Sicherheitsmanagement und Organisation

Ab dem 3. Semester können Sie durch das Auswählen eines Wahlpflichtmodules individuelle Schwerpunkte in den Bereichen IT Infrastruktur, Sicherheitsmanagement und Beratung sowie Malware Analyse setzen.

Der Schwerpunkt **IT-Betrieb** vermittelt Ihnen Zweck und Aufbau von gängigen Betriebssystemen wie Windows und Unix. Sie lernen alles über den Betrieb und Aufbau eines Rechenzentrums, sowie über die notwendige Einbindung der Peripherie. Zusätzlich erstellen Sie zugehörige Sicherheitskonzepte und Sicherungsmechanismen.

Im Schwerpunkt **Netzwerktechnik** beschäftigen Sie sich vor allem mit der Vernetzung von Rechnern, mit Netztopologien und mit den entsprechenden Protokollen. Viel Zeit werden Sie im Labor verbringen, wenn es um die Protokollanalyse und die entsprechenden Tools dafür geht.

All diese Themen bringen Sie weiter, machen Sie zu einer/m Cisco-ExpertIn und vergrößern Ihren Wissensschatz, den Sie für Analysen von Sicherheitslücken und Angriffspotenzialen brauchen.

Mit dem Schwerpunkt **Sicherheitstechnologien** erhalten Sie zuallererst einen Überblick über die Ziele der IT Security und über die gegenwärtigen Bedrohungsszenarien. Zusätzlich erfahren Sie mehr über die kryptografischen Methoden und Werkzeuge. Identifikation und Authentifikation sind ebenfalls wesentliche Bestandteile dieses Bereichs (z.B. Kartensysteme, Biometrie).

Der Schwerpunkt **Sicherheitsmanagement** informiert Sie über Sicherheitsnormen und Standards, über rechtliche Grundlagen und Vertragsrecht. Sicherheits- und Unternehmensmanagement und Wirtschaft runden diesen Schwerpunkt ab.

## Internationalisierung

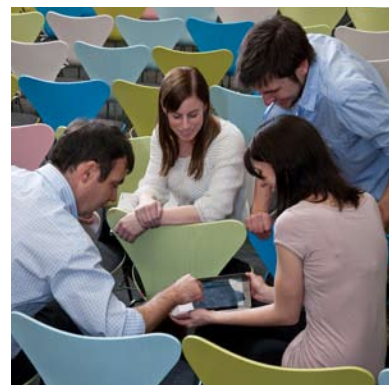
**Knüpfen Sie schon mal internationale Kontakte: Ihr Studium macht es möglich!** Im Rahmen des kostenlosen Intensive Program "Network Security and Forensik" beschäftigen sich Jahr für Jahr 50 Studierende und Lehrbeauftragte aus mehreren europäischen Ländern mit dem Aufspüren, Sichern, Analysieren und Auswerten von verdächtigen kriminellen Handlungen am Computer – der so genannten IT-Forensik.

## Zertifizierungen

Werden Sie marktreif: Sie können während Ihres Studiums unterschiedliche international anerkannte Zertifikate erwerben.

Folgende Zertifikate stehen derzeit zur Auswahl:

- CCNA – Cisco Certified Network Associate
- CCNP – CISCO Career Certifications & Paths
- PHSE – PHION Security Engineer
- MCITP – Microsoft Certified IT Professional
- ITIL V3





## Praxisorientierte Ausbildung

In der letzten Phase Ihres Bachelorstudiums steht der Theorie-Praxis-Transfer im Vordergrund. In zahlreichen Projekten mit Unternehmen und in der so genannten „Krisenwoche“ bereiten Sie sich theoretisch und praktisch auf das Worst-Case-Szenario, den Ernstfall vor. Anhand der Fallstudie „**Business-Continuity und Disaster-Recovery**“ analysieren Sie technische Anforderungen an Systeme (Speichertechnologien, Mirroring). Sie treffen die notwendigen organisatorischen Vorkehrungen und behalten einen kühlen Kopf, wenn es um die Umsetzung in Extremsituationen (Krisenmanagement) geht.

## 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 BetreiberIn.

**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 verhaltenstypische 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.

testete 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

<b>Abschluss:</b>	Bachelor of Science in Engineering (BSc)
<b>Studiendauer:</b>	6 Semester
<b>Organisationsform:</b>	Vollzeitstudium Im Anschluss Masterstudium Information Security möglich
<b>Zahl der Studienplätze/Jahr:</b>	30

Auslandssemester an einer internationalen Partnerhochschule möglich und erwünscht.

## Chancen und Berufsfelder

Ihre Karrierechancen steigen! Wo ein sicherer IT-Betrieb gewährleistet werden muss, sind AbsolventInnen des Bachelorstudiengangs IT Security gefragte MitarbeiterInnen. Ob Industrie, Gewerbe, DienstleisterInnen, Öffentliche Verwaltung etc. Eine Studie zum Thema Security-Software der Gartner Group unterstreicht den Bedarf an AbsolventInnen: Die jährlichen Wachstumsraten in der Security-Branche liegen bei 15 % pro Jahr bis 2012.

AbsolventInnen werden nach entsprechender Berufserfahrung als Führungskräfte sowie als MitarbeiterInnen auf unterschiedlichen Ebenen des mittleren Managements eingesetzt.

## Beispiele aus dem Berufsleben:

Als **Chief Security Officer (CSO)** sind Sie der/die Konzernverantwortliche für den Bereich Sicherheit. Sie beschäftigen sich mit den Bereichen IT- und Informationssicherheit, organisatorische und physische Sicherheit und auch mit elektronischen und mechanischen Sicherheitseinrichtungen. Der CSO ist direkt verantwortlich für die Durchführung, Einhaltung und Entwicklung von sicherheitsrelevanten Themen, die das Unternehmen betreffen.

Wenn Sie als **Netzwerk- und BetriebssystemadministratorIn** tätig sind, befassen Sie sich mit der Administration von Netzwerkkomponenten wie Router, Switch und Firewall. In diesen Bereich fällt auch die Zuständigkeit für einen sicheren und zuverlässigen Betrieb des Netzwerkes. Sie analysieren Logfiles und erkennen frühzeitig Angriffe von außen. Ihr Studium hat Sie fit gemacht, um entsprechende Gegenmaßnahmen zu ergreifen.

Zu den Hauptaufgaben von **IT-ForensikerInnen** gehören IT-Forensische Analysen, die Missbrauchsfälle im Zusammenhang mit elektronischen Systemen rekonstruieren und beweisdienlich dokumentieren. Dies geschieht durch Erfassung, Prüfung und Auswertung digitaler Spuren. Als IT-ForensikerIn erwerben Sie das Wissen, sowohl den Gebrauch als auch den Missbrauch von elektronischen Systemen zu identifizieren. Die zur Untersuchung angewandten Techniken sind allgemein anerkannt. Beweismittel können so gerichtsfest dokumentiert werden.

**Penetration TesterIn:** Das Hauptziel des/der Penetration TesterIn ist Sicherheitsschwachstellen z. B. in Programmen, Web-Applikationen und Computersystemen festzustellen. Als Penetration TesterIn werden Sie dort eingesetzt, wo es gilt, unternehmensweite Sicherheitspolitik, das Sicherheitsbewusstsein der MitarbeiterInnen und die Compliance gegenüber Regulativen zu überprüfen. In diesem Bereich werden Ihre Fachkenntnisse mithelfen, Angriffe von außen und Sicherheitsvorfälle abzuwenden und angemessen darauf zu reagieren.

## Zugangsvoraussetzungen

- Allgemeine Hochschulreife (AHS/BHS) oder
- Ausländische Unireife

### Studieren ohne Matura:

- Berufsreifeprüfung oder
- Studienberechtigungsprüfung oder
- FH-Vorbereitungskurse

„Steig‘ höher ein“: HTL-AbsolventInnen mit facheinschlägiger Vorbildung können ins 2. Semester einsteigen.

## Bewerbung / Aufnahmeverfahren

**Bewerbungsmodus:** schriftlich (mittels Anmeldeformular, Lebenslauf, Nachweis der Zugangsvoraussetzungen -> letztgültiges Abschlusszeugnis, falls z. B. Maturazeugnis noch nicht vorliegt)

**Aufnahmeverfahren:** computergestützter, bildungsneutraler Test und Aufnahmegespräch. Zur weiteren Beurteilung wird auch das letztgültige Abschlusszeugnis herangezogen. Die Aufnahme Termine finden im Sommersemester statt.

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



Mag. Doris Eyett, IMAS International, Marktforschungsinstitut:

„Sieben von zehn IT Verantwortlichen sagen, dass sie prinzipiell Bedarf an derartig ausgebildetem Personal haben.“