



© Raucherbocker Photography

WE ARE **E<sup>3</sup>UDRES<sup>2</sup>**  
EUROPEAN UNIVERSITY

BACHELOR | VOLLZEIT | BERUFSBEGLEITEND | 6/7 SEMESTER

# IT Security

Software Security & Ethical Hacking | Infrastructure, Network & Mobile Security |  
Operating Systems & Cloud Security | Security Management

# IT Security

In einer vernetzten Welt stellen gezielte Cyberangriffe eine massive Bedrohung für Wirtschaft und öffentliches Leben dar. Es braucht daher Expert\*innen, die Organisationen dabei unterstützen, Systeme gegen digitale Gefahren abzusichern und Hackerangriffe abzuwehren. Mit dem Studium IT Security erwerben Sie Skills in den Bereichen Informatik, Management und Teamwork und können so die Herausforderungen von morgen meistern.

## Ihr Studium

Sie erhalten eine 360-Grad-Ausbildung in allen wesentlichen Schwerpunkten der IT Security:

**Infrastructure, Network & Mobile Security:** Studierende erwerben Kenntnisse über Netzwerkprotokolle, Routing und Switching. Darauf aufbauend werden die wichtigsten Hardware-Komponenten und Protokollspezifika behandelt, um Netzwerke sicher zu planen und zu betreiben. Sie lernen die Eigenschaften mobiler Systeme kennen, können Mobile OS Security Features richtig anwenden und Mobile Apps sicher entwickeln.

**Operating Systems & Cloud Security:** Der Schwerpunkt vermittelt Wissen über Betriebssystemarchitekturen. Die Studierenden können danach Windows- und Linux-Systeme administrieren sowie Sicherheitsrisiken erkennen und mitigieren. Ein spezieller Fokus wird auf den Einsatz und die Konfiguration von Betriebssystemen in der Cloud gelegt.

**Software Security & Ethical Hacking:** In diesem Schwerpunkt werden angewandte Programmier- und Datenbankkenntnisse in allen Phasen des Software Development Lifecycles vermittelt. Der Sicherheitsaspekt steht dabei stets im Vordergrund und umfasst das Design, die Umsetzung sowie die statische und dynamische Analyse (Penetration Testing) von Code und (Web-)Applikationen.

**Security Management:** Der Schwerpunkt Sicherheitsmanagement beschäftigt sich mit Sicherheitsnormen und -standards für Unternehmen und umfasst Themen wie die Planung technischer, organisatorischer und menschlicher Abwehrmaßnahmen, das Risiko- und Notfallmanagement sowie rechtlicher Grundlagen rund um Vertragsrecht und Datenschutz.

## Ihre Jobaussichten

Zahlreiche (fächerübergreifende) Projekte in Kooperation mit Unternehmen und Forschungseinrichtungen bereiten Sie auf das Berufsleben vor. Unsere Absolvent\*innen haben eine nahezu 100-prozentige Beschäftigungsquote.

### Berufs- und Tätigkeitsfelder (Auswahl):

- Sicherheitsbeauftragte\*r (Chief Security Officer/ (Chief) Information Security Officer)
- Security-Architekt\*in
- Secure Software Developer
- IT Forensiker\*in
- Security Cloud Specialist
- Security-Berater\*in
- Netzwerk-/Betriebssystem-Administrator\*in
- Datenschutzbeauftragte\*r
- Auditor\*in
- Business Continuity Analyst\*in oder Manager\*in
- System, App, Network/Web Penetration Tester\*in
- Incident Responder



© Rauchecker Photography



### Abschluss

Bachelor of Science  
in Engineering (BSc)



### Studiendauer

6/7 Semester



### Studiengebühren

363,36 € pro Semester  
+ ÖH-Beitrag



### Bewerbung & Aufnahmeverfahren

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



### Studienplätze/Jahr

35 Vollzeit  
15 berufsbegleitend



### Organisationsform

Vollzeit (6 Semester)  
berufsbegleitend (7 Semester)

# Das macht Ihr Studium einzigartig

## Verknüpfung mit der Forschung

Durch die enge Verknüpfung mit dem Institut für IT Sicherheitsforschung und dem Josef Ressel Zentrum für Blockchain-Technologien & Sicherheitsmanagement stellen wir den Bezug zwischen Studium, aktuellen Themen sowie künftigen Entwicklungen der IT Security sicher.

## Praxisnaher Unterricht & starke Vernetzung

Ein wesentlicher Teil der Ausbildung ist die Praxisnähe. In zahlreichen Projekten mit Unternehmen und in der „Krisenwoche“ bereiten Sie sich theoretisch und praktisch auf eine Vielzahl von Einsatzszenarien vor. In unserem Cyber Defense Center (CDC) erwerben Sie wichtige Kompetenzen rund um das Entdecken und Analysieren von schädlicher Aktivität in Netzwerken und Betriebssystemen. Zudem profitieren Studierende von einer engen Vernetzung mit Expert\*innen aus der Praxis – sei es im Rahmen von Gastvorträgen oder bei kostenlosen Konferenzbesuchen.

## Innovative Lehrmethoden

Innovatives Lernen kennt bei uns keine Grenzen. Lehrveranstaltungen werden in zusammenhängenden Blockeinheiten unterrichtet – so können Sie schnell in aktuelle

Themen eintauchen. In Inverted Classrooms oder beim Game Based Learning trainieren Sie Ihre Fähigkeiten in spielerischer Umgebung.

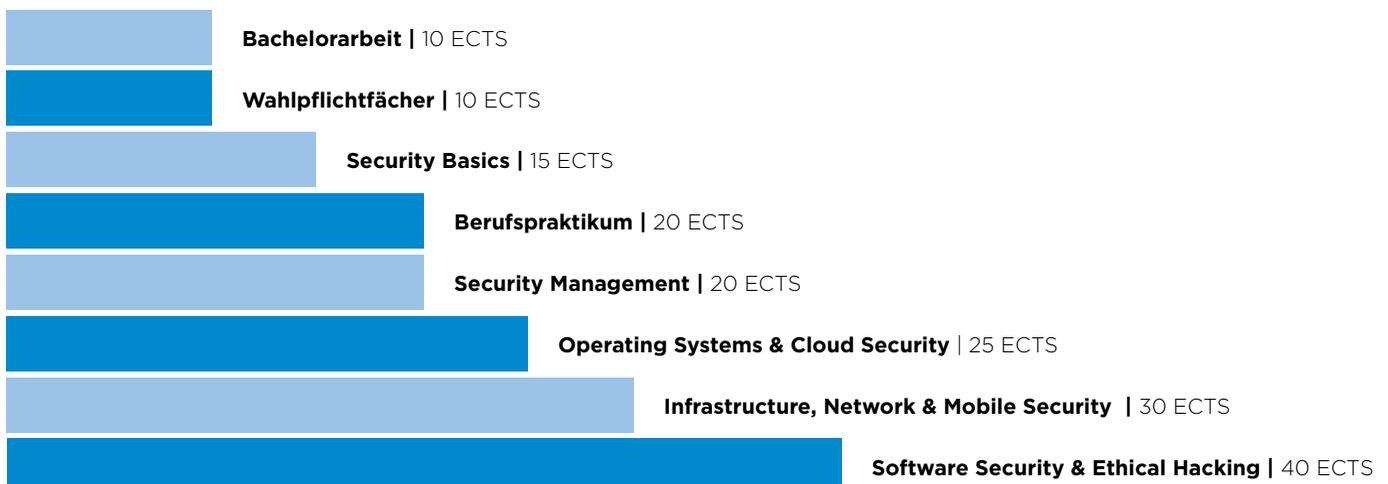
## Moderne Infrastruktur

Für die Durchführung einer praxisorientierten Ausbildung stehen Ihnen 5 unabhängige Labore mit modernster PC- und Virtualisierungsinfrastruktur zur Verfügung. Sie können die gesamte Infrastruktur rund um die Uhr nutzen, auch von Zuhause aus.

## Studium und Beruf

Der Studiengang ist bestmöglich auf die Bedürfnisse von Berufstätigen abgestimmt – auch als Vollzeitstudium. Online-Lehrveranstaltungen machen etwa 20 Prozent des Studienplans aus, der Unterricht findet von Montag bis Donnerstag statt. Beim berufsbegleitendem Studium findet der Unterricht Donnerstagabend online sowie Freitagnachmittag und Samstag in Präsenz statt. Die verpflichtenden Berufspraktika (12 Wochen) können über die gesamte Studiendauer verteilt absolviert werden. Studierenden, die bereits facheinschlägig arbeiten, wird das Praktikum angerechnet.

## Gewichtung der Studieninhalte



# Studienplan (berufsbegleitend)

## 1. Studienjahr

1. Semester	ECTS
Team Training and Conversation	5
Mathematics for Security Experts	5
Introduction to Networks and Distributed Systems	5
Windows Administration	5
OS Fundamentals & Linux Security	5

## 2. Semester

2. Semester	ECTS
Building Computer Networks	5
Network Protocols	5
Cryptography	5
Coding Basics	5

## 2. Studienjahr

3. Semester	ECTS
Networking Security	5
Secure Coding & Database Fundamentals	5
Advanced Coding & Database Technologies	5
Sicherheitsmanagement 1 – ITIL, Basics und Systeme	5
Sicherheitsmanagement 2 – Code of Practice	5
Berufspraktikum	4

## 4. Semester

4. Semester	ECTS
Introduction CDC	5
Secure Software Engineering	5
Web and Application Security	5
Digital Forensics	5
Sicherheitsmanagement 3 – Risiko und Notfall	5
Berufspraktikum	4

## 3. & 4. Studienjahr

5. Semester	ECTS
Mobile Systems and Authentication	5
Essential Hacking Tools & Penetration Testing	5
Introduction to Research Practices and Scientific Writing	5
Operating Systems Hardening	5
Berufspraktikum	4

## 6. Semester

6. Semester	ECTS
Cloud Computing & Cloud Security	5
Security Architecture	5
Wahlpflichtfach	10
Berufspraktikum	4
Sicherheitsmanagement 4 – Outsourcing	5

## 7. Semester

7. Semester	ECTS
Business Continuity	5
Bachelorarbeit mit Bachelorseminar	10
Security Project	5
Berufspraktikum	4

# Studienplan (Vollzeit)

## 1. Semester

1. Semester	ECTS
Team Training and Conversation	5
Mathematics for Security Experts	5
Introduction to Networks and Distributed Systems	5
Coding Basics	5
Windows Administration	5
OS Fundamentals & Linux Security	5

## 2. Semester

2. Semester	ECTS
Building Computer Networks	5
Network Protocols	5
Cryptography	5
Secure Coding & Database Fundamentals	5
Sicherheitsmanagement 1 - ITIL, Basics und Systeme	5
Sicherheitsmanagement 2 - Code of Practice	5

## 3. Semester

3. Semester	ECTS
Network Security	5
Introduction CDC	5
Secure Software Engineering	5
Web and Application Security	5
Advanced Coding & Database Technologies	5
Sicherheitsmanagement 3 - Risiko und Notfall	5

## 4. Semester

4. Semester	ECTS
Mobile Systems and Authentication	5
Essential Hacking Tools & Penetration Testing	5
Digital Forensics	5
Operating Systems Hardening	5
Cloud Computing & Cloud Security	5
Sicherheitsmanagement 4 - Outsourcing	5

## 5. Semester

5. Semester	ECTS
Berufspraktikum	20
Security Project	5
Introduction to Research Practices and Scientific Writing	5

## 6. Semester

6. Semester	ECTS
Business Continuity	5
Security Architecture	5
Wahlpflichtfach	10
Bachelorarbeit mit Bachelorseminar	10

Das verpflichtende Berufspraktikum im Umfang von 20 ECTS kann über die gesamte Studiendauer verteilt absolviert werden. ECTS: European Credit Transfer System – Maß für den gesamten Arbeitsaufwand für durchschnittliche Studierende, um eine Lehrveranstaltung positiv zu absolvieren. Ein Leistungspunkt (oder Credit Point) steht für 25 Stunden Arbeitsaufwand (Präsenzzeiten, Selbststudium, Prüfungen etc.).

Alle Details und Informationen zu  
**IT Security**





© Raucherker Photography

## Information & Kontakt

Campus und Study Center (CSC) | T: +43 2742 313 228-333 | E: [csc@fhstp.ac.at](mailto:csc@fhstp.ac.at) | I: [fhstp.ac.at](http://fhstp.ac.at)

## Diversität am Campus St. Pölten

Alle sind willkommen: Inklusion, Geschlechtergerechtigkeit und Vielfalt sind uns wichtig. Unser Campus ist barrierefrei zugänglich. Bitte nehmen Sie rechtzeitig mit uns Kontakt auf, damit wir Ihre Bedürfnisse berücksichtigen können.