Fernfachhochschule Schweiz
Zürich | Basel | Bern | Brig

Mitglied der SUPSI

Informationssicherheit

Code	ISich			
Fachbereich(e)	Informationssicherheit			
Studiengang /-gänge	BSc Informatik, BSc Wirtschaftsinformatik, MAS Web4Business			
Vertiefungsrichtung(en)	-			
Art des Studiengangs	☒ Bachelor	☐ Master	☒ CAS/MAS/EMBA	
Studienniveau *	☒ Basic	☐ Intermediate	☐ Advanced	☐ Specialised
Typus **	☒ Core course	☐ Related course	☐ Minor course	
ECTS-Credits	5			
Präsenzverpflichtung	20 Lektionen			
Arbeitsaufwand in Std.	150			
Verantwortliche Ansprechperson	Fachbereichsleiter: Josef Schuler	Autor: Christian Thiel / Thomas Punz		
Zu entwickelnde Kompetenzen	Die Studierenden erlernen die Denkweise, Begriffe und Methoden der Informationssicherheit. Sie wissen, welche Bedrohungen existieren und mit welchen Massnahmen diese gemildert werden können. Nebst dem theoretischen Fundament vertiefen die Studierenden durch HackingTool Übungen mit verwundbaren Anwendungen und Systemen die erlernten Grundlagen und können dadurch sowohl selbstständig Angriffsszenarien nachbilden wie auch Gegenmassnahmen entwickeln. In Gruppenarbeiten wird die Fähigkeit, gemeinsam Lösungen zu entwickeln und verschiedene Rollen einzunehmen, gefördert. Die Studierenden können das erlernte Wissen in einen neuen Kontext übertragen und dort anwenden.			
Lerninhalte	• Grundlagen und die relevanten Begriffe der IT-Sicherheit • Kenntnis der aktuellen Bedrohungen • Implementierung von angemessenen sicherheitstechnischen Massnahmen im IKT-Umfeld einer Firma basierend auf den formulierten Sicherheitsanforderungen und den Geschäftsprozessen • Fokus auf die Themengebiete Anwendungssicherheit, Kryptographie, Identity und Access Management, System- und Netzwerksicherheit • HackingTool Übungen zu ausgewählten Angriffsvektoren			
Lehr- und Lernmethoden (Fernstudium nach dem Blended-Learning-Konzept)	Selbststudium • Erarbeiten des Stoffes • Lektüre • Lösen von Aufgaben • Lesen von Security News Tickern	Online-Studium • Forumsdiskussionen • Einreichen von Aufgaben • Repetitionsaufgaben • HackingTool Übungen	Präsenzstudium • Lehrgespräch • Demonstrationen von Angriffsvektoren • Gruppendiskussionen • Präsentationen • Fragerunden	
Unterrichtssprache	Deutsch			
Leistungsbewertung	20% Übungen (als Semesterarbeit in Gruppen), 80% schriftl. Modulprüfung			
Lehrmittel	Eckert, C.: IT-Sicherheit: Konzepte – Verfahren, Oldenbourg Wissenschaftlicher Verlag; ISBN: 978-3486778489, 9. Auflage 2014. Schuler, J.: Einführung in die Kryptographie, online auf Moodle			
Vorkenntnisse: Modul(e)	GMath, DMathLS, GInf, PVANV			
Anschlussmodul(e)	M-ITSec, INSich, Krypt			
Bemerkungen	-			

*Studienniveau	**B** Basic level course: Modul zur Einführung in das Basiswissen eines Gebiets. **I** Intermediate level course: Modul zur Vertiefung der Basiskenntnisse. **A** Advanced level course: Modul zur Förderung und Verstärkung der Fachkompetenz. **S** Specialised level course: Modul zum Aufbau von Kenntnissen und Erfahrungen in einem Spezialgebiet.
**Typus	**C** Core course: Modul des Kerngebiets eines Studienprogramms. **R** Related course: Unterstützungsmodul zum Kerngebiet (z.B. Vermittlung von Vor- oder Zusatzkenntnissen). **M** Minor course: Wahl- oder Ergänzungsmodul.

1 Stoffplan

Der Grundkurs ist technisch ausgerichtet. Nach einer Einführung in die Informationssicherheit und einem Kennenlernen der aktuellen Bedrohungen, folgen Lektionen die aufzeigen, wie man in jedem Umfeld (KMU, Verwaltung, grössere Unternehmungen) mit geeigneten Mitteln die IT-Sicherheit verbessern und umsetzen kann. Die Massnahmen sind stets von Übungen und Demonstrationen begleitet, welche zuerst den Angriff aufzeigen und die Studierenden danach mögliche Gegenmassnahmen bestimmen lassen.

Einführung in die Informationssicherheit und Sicherheitskonzepte

- Ausgangslage
- Einige aktuelle Bedrohungen
- Grundlagen und Begriffe
- Einführung in die HackingTool Übungen

Anwendungs-Sicherheit

- Typische Attacken auf Webanwendungen
- OWASP Top 10 vorstellen mit Demonstrationen und Übungen
- Sicheres Programmieren
- Vom Test zur Produktion am Beispiel des Security Development Life Cycles von Microsoft

Einführung in die Kryptographie und Anwendung in der Praxis

- Kurze Einführung in die Kryptographie
- Symmetrische und asymmetrische Verschlüsselung
- Hashfunktionen
- Digitale Signaturen
- Übungen und Demonstrationen

Identity und Access Management

- Treiber für das Thema IAM
- Prozesse im Bereich IAM mit Fokus auf das Provisioning von Identitäten
- Authentisierung und Autorisierung
- Identity Federation
- Übungen und Demonstrationen

Netzwerk- und Systemsicherheit

- Bedrohungen der Netzwerksicherheit
- Netzwerksegmentierung, Firewalls und Intrusion Detection
- Bedrohungen der Systemsicherheit
- Demonstration von Metasploit
- Logfile Analyse
- Patching und Hardening