Modulbeschrieb

Information Security

Modulcode	M20
Leitidee	Die Informations- und Kommunikationstechnologie spielt eine zentrale Rolle für das Funktionieren moderner Wirtschaftssysteme. Ihre Allgegenwart und die Selbstverständlichkeit ihres Einsatzes erfordert gezielt und korrekt eingesetzte Massnahmen der IT-Sicherheit, um die Risiken wirtschaftlicher Schäden durch externe Angriffe oder internen Missbrauch zu reduzieren. In diesem Modul werden grundlegende Kenntnisse über die Verfahren und Protokolle vermittelt, mit denen die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellt werden können. Der Studierende entwickelt ein Bewusstsein für IT-Sicherheitsrisiken, welches den Schutz persönlicher Daten einschliesst, und erlangt ein breites und grundlegendes Wissen zu deren Begrenzung.
Art der Ausbildung	Wirtschaftsinformatik
Studiengang	Master of Science
Modultyp	Wahlpflichtmodul
ECTS Dotation	3 Credits
Für Modul verantwortlich	Prof. Dr. Günter Karjoth, Hochschule Luzern
Eingangskompetenzen	-
Anschlussmodule	-
Bemerkungen	-

Ausgangskompetenzen / Grobziele

Die Studierenden verstehen die Bedeutung der behandelten Modelle und Methoden der Informationssicherheit und können sie zum Schutz von betrieblichen und personenbezogenen Daten sachgerecht einsetzen.

Sie können Informationen aus der Berichterstattung über IT-Sicherheitsvorfälle einordnen, sich selbständig in ein aktuelles IT-Security-Thema einarbeiten und ihre Erkenntnisse angemessen kommunizieren.

Die Studierenden erarbeiten sich ein Verständnis der Schutzmassnahmen in den Themenbereichen Identitäts-Management, Zugriffskontrolle, Netzwerk- und Applikationssicherheit, Sicherheit mobiler Anwendungen und Datenschutz.

Sie können die Bedrohungen der Informationssicherheit, welche mit gesellschaftlichen Veränderungen wie Web 2.0, allgegenwärtiger Vernetzung, steigender Mobilität und dem „Internet der Dinge“ einhergehen, einordnen.

Ziele

Fachkompetenz

Die Studierenden

- verstehen die Konzepte zur Authentisierung und Autorisierung angewandt in ihrem beruflichen Umfeld,
- verstehen Firewall- und VPN-Konzepte und können bei deren Planung eine aktive Rolle spielen,
- verstehen die Konzepte des Datenschutzes und Massnahmen zu dessen Erfüllung,
- können den Umfang und die Qualität von Sicherheitsprodukten und -dienstleistungen bewerten und kennen unterschiedliche Ansätze zur Risikoverminderung,
- können das gelernte Wissen auf neue Technologien übertragen (z. B. mobile & eingebettete Systeme).

Methodenkompetenz

Die Studierenden

- wissen die behandelten Methoden zum Schutz von Daten in ihrem eigenen Arbeitsgebiet einzusetzen,
- recherchieren selbständig und zielorientiert zu einem vorgegebenen Thema oder einer vorgegebenen Problemstellung.

Sozial-/Selbstkompetenz

Die Studierenden

- pflegen einen bewussten und verantwortungsvollen Umgang mit der (eigenen und fremden) Privatsphäre
- wissen um die Bedeutung der Privatsphäre im Kontext der allverfügbaren Kommunikationsmittel.

Lerninhalte

Schwerpunkt „Kontext und Konzepte“

- Schutzziele
- Schwachstellen, Bedrohungen und Angriffe
- Richtlinien und Massnahmen

Schwerpunkt „Authentifikation“

- Passwörter, Biometrie, Security Tokens, Single Sign-On
- Identity Management

Schwerpunkt „Sicherheitsmodelle und Zugriffskontrolle“

- Zugriffskontrolllisten, Bell-LaPadula- und Chinese-Wall-Modell
- Rechteverwaltung und Rechteprüfung
- Rollenkonzepte, Role Engineering (Role Mining, Rollenqualität)

Schwerpunkt „Schlüsselmanagement“

- Schlüsselerzeugung, -aufbewahrung und -austausch
- Zertifizierung, Public-Key Infrastruktur

Schwerpunkt „Netzwerksicherheit“

- Firewalls, sichere Kommunikation und sichere Anwendungsdienste
- VPN, Firewall-Konzepte, Intrusion Detection Systems (IDS)
- SAML, OAuth 2.0, DDoS
- WLAN, Bluetooth, RFID & NFC

Schwerpunkt „Sicherheit in Anwendungen“

- Datenbanksicherheit, SQL Injection
- Testdatenmanagement

Schwerpunkt „Kryptographische Grundlagen“

- Zufallszahlen, Hashfunktionen, symmetrische und asymmetrische Verschlüsselung, digitale Signaturen

Schwerpunkt „Datenschutz"

- Zweckbestimmung, Zustimmung, Anonymität

ECTS Credits	Kontaktstudium (Lektionen)	Kontaktstudium (Stunden)	Begleitetes Selbststudium (Lektionen)	Begleitetes Selbststudium (Stunden)	Autonomes Selbststudium (Stunden)	**Total (Stunden)**
3	28	20.0	46	34.0	36.0	**90**
		22.2%		37.8%	40.0%	**100%**

Lehr- und Lernformen

Kontaktstudium	Dialogorientierter Unterricht mit aktuellen Beispielen
Selbststudium	Übungen zur Vertiefung und Anwendung der erlernten Theorie, Problem-based learning

Unterrichtssprache Deutsch

Leistungsnachweis/e

Anzahl	Art des Leistungsnachweises	Gewichtung	Dauer	Hilfsmittel
1	Modulschlussprüfung	100%	60 Min.	Closed Book

Präsenzpflicht -

Bibliographie Deutsch oder Englisch

Empfohlene Literatur:

- Eckert, Claudia. IT-Sicherheit. 9. Aufl. Oldenbourg Verlag 2014.
- Ergänzende Literatur (Bücher, Artikel) wird durch den Dozierenden fallspezifisch empfohlen.