Modul: IT-Security & IT-Risk Management

Semester: 5
Modulverantwortlicher: Prof. Dr. Koch,
Code der Veranstaltung: SRM
Unterrichts-/Lehrsprache: Deutsch
ECTS Punkte: 5
Kontaktstunden: 40
Selbststudium: 110
Dauer des Moduls: 1 Semester
Häufigkeit des Angebots des Moduls:
Entsprechend dem Studienplan der Gruppen
Gewichtung der Note in der Gesamtnote: 2,91%
Art und Umfang der Prüfungsleistung: KRS90 = Die Prüfung besteht **entweder** aus einer Klausur **oder** einem Referat **oder** einer Studienarbeit; im Fall einer Klausur gibt die Zahl den Umfang der Klausur in Minuten

Teilnahmevoraussetzungen:
Mathematische Grundvorlesung, Grundlagen der Informatik, Einführung in die Wirtschaftsinformatik, Requirements Engineering, Projekt- und Teammanagement, Projekte der Wirtschaftsinformatik, Grundlagen im Bereich Netze und Betriebssysteme

Verwendbarkeit des Moduls für andere Module und Studiengänge:
Verwendbar für das Modul Unternehmensethik sowie konsekutive IT-Master Studiengänge

Qualifikations- und Kompetenzziele:
Die Studierenden erlangen einen vertieften Einblick in die Bereiche IT-Sicherheit und IT-Risk-Management, wodurch sie befähigt werden, die erlernten Erkenntnisse praxisrelevant und anwendungsorientiert einzusetzen. Es werden Kenntnisse vermittelt, die dazu dienen IT-Sicherheit und IT-Risikomanagement als interdisziplinäre und interdependente Unternehmensaufgabe bzw. Herausforderung aufzufassen. Die Studierenden beherrschen die Grundkonzepte der IT-Sicherheit und kennen Methodiken zur Ermittlung von Sicherheitsanforderungen, Erstellung von Sicherheitsanalysen und daraus abgeleiteten Sicherheitskonzepten.

Kryptographische Basismechanismen, Netzwerksicherheit, Anwendungssicherheit und Sicherheit für multimediale Anwendungen und Daten bilden wesentliche fachliche Grundbausteine des Moduls. Die Studierenden kennen unterschiedlichste Aspekte sicherheitsrelevanter Systeme und deren Bezug zu konkreten Anwendungen. Neben technischen Aspekten werden auch Fragen des Sicherheitsmanagements betrachtet. Darüber hinaus verstehen die Studenten die Grundprinzipien des IT-Risiko-Managements, wozu insbesondere die Bedrohungs- und Risikoanalyse zählen. Sie haben erfahren wie Risiko-Einschätzungen vorgenommen werden und können Gegenmaßnahmen identifizieren und bewerten. Risiko-Management wird als kontinuierlicher Prozess verstanden, der in die Unternehmensabläufe und Strategien des Unternehmens integriert ist.

Lehr- und Lernmethodik:
Klassischer Vortrag, Durchführung von Übungen mit Präsentation der Ergebnisse, Fallstudienarbeit, praktische Übungen

zu Modul: IT-Security & IT-Risk Management

Inhalte des Moduls:

1. Grundlagen der IT-Sicherheit
   1.1 Wachsende Bedeutung des Themas IT-Sicherheit
   1.2 Gesetzliche Anforderungen und Bezug zur Risikomanagement

2. Kryptographische Grundlagen und Sicherheitsprotokolle
   2.1 Hash-Verfahren, Verschlüsselungsverfahren
   2.2 Public-Key Verfahren
   2.3 Key-Management und Public-Key Infrastrukturen

3. Sicherheit für verschiedene Ebenen und Anwendungen
   3.1 Netzwerk- und Betriebssystemsicherheit
   3.2 Sicherheit von Anwendungen
   3.3 Schutz von multimedialen Daten
   3.4 Fakultativ ausgewählte Anwendungen und Praxisbeispiele

4. Zyklus der Informationssicherheit
   4.1 Sicherheitsanforderungen
   4.2 Sicherheitsanalyse
   4.3 Sicherheitskonzepte
   4.4 Umsetzungsbeispiele und ggf. zugehörige Übungen

5. Nationale und internationale IT-Sicherheitsframeworks, Evaluationskriterien
   5.1 BSI Grundschutz,
   5.2 ISO 27001 – 5
   5.3 Evaluation von Sicherheit nach ITSec und Common Criteria

6. IT-Risikomanagement als Prozess in Unternehmen
   6.1 Grundlagen und Begriffe sowie Einordnung im Unternehmenskontext
   6.2 Zyklus des Risikomanagements

Literatur:

- Eckert, Claudia: IT-Sicherheit: Konzepte – Verfahren – Protokolle, Oldenbourg 2009
- Anderson, Ross: Security Engineering, Wiley, 2008
- Schneier, Bruce: Angewandte Kryptographie, Pearson, 2005
- Schmehl, Klaus: Kryptographie, dpunkt, 2007
- Königs: IT-Risiko-Managment mit System, vieweg, 2006
- Peltier: Information Security Risk Analysis, CRC Press, 2010
- Dieter Burgartz / Ralf Röhrig (Hrsg.), TÜV Media: Information Security Management. Praxishandbuch für Aufbau, Zertifizierung und Betrieb
- Alan Calder & Steve Watkins: International IT Governance: An Executive Guide to ISO 17799 / ISO 27001