

Modulbeschreibung

IT-Security

Allgemeine Informationen
Anzahl ECTS-Credits

3

Modulkürzel

TSM_ITSec

Version

16. Juli 2010

Modulverantwortliche/r

Marc Rennhard, ZHAW

Sprache

	Lausanne	Bern	Zürich
Unterricht	<input type="checkbox"/> E <input checked="" type="checkbox"/> F	<input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F	<input checked="" type="checkbox"/> D <input checked="" type="checkbox"/> E
Unterlagen	<input checked="" type="checkbox"/> E <input type="checkbox"/> F	<input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F	<input type="checkbox"/> D <input checked="" type="checkbox"/> E
Prüfung	<input checked="" type="checkbox"/> E <input type="checkbox"/> F	<input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F	<input type="checkbox"/> D <input checked="" type="checkbox"/> E

Modulkategorie

- Erweiterte theoretische Grundlagen
- Technisch-wissenschaftliche Vertiefung
- Kontextmodule

Lektionen

- 2 Vorlesungslektionen und 1 Übungslektion pro Woche
- 2 Vorlesungslektionen pro Woche

Kurzbeschreibung /Absicht und Inhalt des Moduls in einigen Sätzen erklären

Dieses Modul vermittelt die wesentlichen Konzepte und Technologien der IT-Security. Behandelt werden die gegenwärtigen Sicherheitsbedrohungen, Sicherheitstechnologien, sichere Software- und Systementwicklung sowie Sicherheitstests. Die Studierenden erwerben die Grundlagen für das Entwerfen sicherer Systeme und der Implementierung und Beurteilung von IT-Security auf Unternehmensebene.

Ziele, Inhalt und Methoden
Lernziele, zu erwerbende Kompetenzen

- Die Studierenden kennen die gegenwärtigen Sicherheitsbedrohungen im IT-Bereich
- Die Studierenden kennen die gebräuchlichen Methoden, Technologien und Tools der IT-Sicherheit
- Die Studierenden sind in der Lage, diese Werkzeuge und Methoden in der Realität anzuwenden
- Die Studierenden wissen, wie sichere Software und Systeme entwickelt werden und was für Techniken dafür existieren
- Die Studierenden wissen, wie Software und Systeme auf ihre Sicherheit geprüft werden

Modulinhalt mit Gewichtung der Lehrinhalte

Das Modul besteht aus 4 Hauptthemen:

- Sicherheitsziele und Überblick über häufige Bedrohungen
 - Definition von IT-Security, Sicherheitsziele: CIA, AAA
 - Typische gegenwärtige Angriffe: Malware (Viren, Würmer, Trojanische Pferde), Passwörter und Probleme, Phishing, kompromittierte Systeme, (D)DoS-Angriffe, Angriffe auf Webapplikationen (XSS, SQL Injection), Buffer-Overflow-Angriffe, organisierte Cyberkriminalität
- Sicherheitstechnologien
 - Etablierte, fortgeschrittene Sicherheitstechnologien: Access-Control-Mechanismen, Federated Identities, Betriebssysteme, Application-Layer-Firewall, Intrusion Detection/Prevention Systeme
- Entwicklung sicherer Software und Systeme
 - Konzepte für die sichere Programmierung: Konzepte für sichere und robuste Programmierung, Security Patterns, Tools um die Robustheit/Sicherheit von Programmen zu erhöhen
 - Sicherheit von Webapplikationen und Web-Services: Typische Sicherheitsprobleme in Webapplikationen, Sicherung von

Webapplikationen, Sicherheit von Web-Services

- Testen von Software- und Systemsicherheit
 - Penetration Test einer Webapplikation als Beispiel für einen Sicherheitstest: verschiedene Phasen des Penetration Tests, manuelle Methoden und Tools, testen von Web Applikationen und ausnützen von Schwachstellen

Lehr- und Lernmethoden

- Vorlesungen
- Übungen und Selbststudium: Praktische Übungen am Computer, Theorieübungen

Voraussetzungen, Vorkenntnisse, Eingangskompetenzen

Es wird vorausgesetzt, dass die Studierenden Grundkenntnisse in Kryptologie und eine Grundlage im Bereich der sicheren Kommunikationsprotokolle besitzen (entspricht ungefähr einem 4 ECTS Bachelormodul). Siehe z. B: Network Security: Private Communication in a Public World, Second Edition Charlie Kaufman, Radia Perlman, Mike Speciner, 2nd Edition. Ebenfalls wird vorausgesetzt, dass die Studierenden fundierte Kenntnisse in mindestens einer modernen Programmiersprache wie Java, C oder ähnlich aufweisen.

Bibliografie

Vorlesungsunterlagen der Dozenten, Verweise auf Internetquellen und Fachliteratur

Leistungsbewertung

Zulassungsbedingungen für die Modulschlussprüfung (Testatbedingungen)

Schriftliche Modulschlussprüfung

Prüfungsdauer : 120 Minuten
Erlaubte Hilfsmittel: Sämtliche Unterlagen und Notizen, keine elektronischen Geräte