

Modul für den Studiengang Informatik / Softwaretechnik

Modulbezeichnung	Sicherheit
Kürzel für Stundenplan	Sic
Semester	6
Modulverantwortliche(r)	Prof. Dr.-Ing. H. Hinrichs
Dozent(in)	Prof. Dr.-Ing. H. Hinrichs
Sprache	Deutsch
Zuordnung zum Curriculum	Bachelor-Studiengang Informatik
Lehrform/SWS	2 V mit integrierten Übungen, 2 P am Rechner
Arbeitsaufwand	V 32h plus die Hälfte für Vor-/Nachbereitung = 48h P 32h plus das Zweifache für Vor-/ Nachbereitung = 96h
Kreditpunkte	5 cp
Voraussetzungen	Kenntnisse in Programmierung, Rechnernetzen, Betriebssystemen
Lernziele/Kompetenzen	<p>Die Studierenden lernen in diesem Modul, dass IT-Sicherheit mehr umfasst als Virens Scanner und Firewalls. Ausgehend von einem Überblick über die verschiedenen Sicherheitskonzepte wird Ihnen deutlich gemacht, dass IT-Sicherheitsmaßnahmen nur dann wirksam vor Angriffen schützen können, wenn sie zu einer in sich stimmigen Gesamtlösung integriert werden. Außerdem werden die Studierenden nach dem Absolvieren dieses Moduls die wichtigsten Angriffstechniken kennen sowie im Hinblick auf die von ihnen ausgehenden Bedrohungen und auf zu ergreifende Gegenmaßnahmen einordnen können. Auf konzeptioneller Ebene wird anhand praktischer Beispiele vermittelt, wie eine gegebene IT-Infrastruktur systematisch auf Schwachstellen hin untersucht werden kann, um im zweiten Schritt ihren Schutzbedarf festzustellen und mit adäquatem Aufwand einen sog. „Grundschutz“ zu etablieren.</p> <p>Die theoretischen Konzepte werden durch begleitende praktische Aufgaben vertieft. Dabei sammeln die Studierenden Erfahrungen mit einer Reihe von (frei verfügbaren) Softwarewerkzeugen, die sich in der Praxis als Bestandteile von IT-Sicherheitslösungen bewährt haben. Sie sind somit anschließend in der Lage, diese Werkzeuge zielgerichtet zu konfigurieren und einzusetzen.</p>
Inhalt	Siehe unten
Studien-/Prüfungsleistungen	Mündliche Prüfung
Medienformen	Beamerpräsentation, Skript, Übungsblätter
Literatur	<ul style="list-style-type: none"> • Schneier, B. Secrets & Lies, dpunkt, 2004. • Northcutt, S. et al. Network Perimeter Security,

New Riders, 2003.

- Schäfer, G. Netzsicherheit, dpunkt, 2003.
- Aurand, A. LAN-Sicherheit, dpunkt, 2004.

Studieninhalte des Moduls **Sicherheit**

1. Motivation und Einführung

2. Angriffstechniken

- Aktive Angriffe
 - Password Cracking
 - Denial of Service
 - Tarnung (Spoofing)
 - Viren, Würmer und Trojaner
 - Ausnutzung programmiertechnischer Schwachstellen
- Passive Angriffe
 - Mitlesen von Nachrichten (Sniffing)
 - Analyse der technischen Infrastruktur (Scanning)

3. Konstruktion sicherer Systeme

- IT-Grundschutzhandbuch
- IT-Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung nach IT-Grundschutz
- Basis-Sicherheitscheck

4. Firewalls

- Paketfilter
- Application Gateways
- Proxies
- Firewall-Architekturen

5. Abhärtung von Routern und Servern

6. Intrusion Detection Systems

- Ziele und Funktionsweise
- Probleme beim Einsatz von IDS

7. Digitale Forensik

- Vorgehensweise
- Werkzeuge

8. Sicherheitsprotokolle für den OSI-Stack

- IPSec
- SSL

9. Zugriffskontrolle