Modul BA-INF 136	**Reaktive Sicherheit**		
Workload 180 h	**Umfang** 6 LP	**Dauer** 1 Semester	**Turnus** jährlich
Modulverantwortlicher	Prof. Dr. Michael Meier		
Dozenten	Prof. Dr. Michael Meier		
Zuordnung	**Studiengang** B. Sc. Informatik	**Modus** Wahlpflicht	**Studiensemester** 4. oder 6.
Lernziele: fachliche Kompetenzen	Die Veranstaltung stellt dar, wo das Präventionsparadigma zu kurz greift und motiviert ergänzende Maßnahmen für eine reaktive Sicherheit. Die Hörer werden für Verwundbarkeiten informationstechnischer Systeme sowie deren Entstehung bei der Entwicklung und beim Betrieb sensibilisiert. Darüber hinaus wird in die Erkennung und Analyse vorhandener Verwundbarkeiten sowie von Schadsoftware und Angriffen eingeführt. Einschlägige ausgewählte Techniken werden erläutert und ausgewählte Werkzeuge beschrieben. Wechselwirkungen mit dem Datenschutz werden aufgezeigt.		
Lernziele: Schlüsselkompetenzen	Den Studierenden sollen Ursachen für Verwundbarkeiten bewusst werden. Sie sollen Techniken zum Umgang mit verwundbaren Systemen beherrschen. Dabei sollen Ansätze von Angreifern und Schadsoftware kennengelernt werden. Die Studierenden sollen methodische Kenntnisse zur Analyse von Schadsoftware und Angreifertechniken sowie zur Erkennung von Verwundbarkeiten und deren Ausnutzung erwerben und anwenden können. Außerdem sollen die Studierenden ausgewählte Techniken zur Balance von Überwachungs- und Datenschutzinteressen kennen lernen.		
Inhalte	• Präventive IT-Sicherheit • Passwort-basierte Authentifikation • Netzverwundbarkeiten • Programm- und Web-Verwundbarkeiten • Malware • Tarntechniken und Rootkits • Honeypots • Intrusion Detection • Datenschutzaspekte		
Teilnahmevoraussetzungen	**Empfohlen:** alle Module aus folgender Liste: BA-INF 101 – Kommunikation in Verteilten Systemen BA-INF 034 – Systemnahe Programmierung BA-INF 138 – IT-Sicherheit		

Veranstaltungen

Lehrform	**Gruppengröße**	**SWS**	**Workload[h]**	**LP**
Vorlesung	40	2	30 P / 45 S	2,5
Übungen	20	2	30 P / 75 S	3,5

P = Präsenzstudium, S = Selbststudium

Prüfungsleistungen	Schriftliche Prüfung	(benotet)
Studienleistungen	Erfolgreiche Übungsteilnahme	(unbenotet)
Medieneinsatz		
Literatur	• John Aycock. Computer Viruses and Malware. Springer, 2006. • Michael Meier. Intrusion Detection effektiv! Modellierung und Analyse von Angriffsmustern. X.systems.press, Springer, 2007. • Niels Provos und Thorsten Holz: Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison Wesley, 2007.	