Modulbezeichnung	IT-Forensik
Modulbezeichnung (eng.)	IT Forensics
Semester (Häufigkeit)	5 (jedes Wintersemester)
ECTS-Punkte (Dauer)	5 (1 Semester)
Art	Pflicht
Studentische Arbeitsbelastung	25 h Kontaktzeit + 125 h Selbststudium
Voraussetzungen (laut BPO)	
Empf. Voraussetzungen	
Verwendbarkeit	BOMI
Prüfungsform und -dauer	Klausur (120 min.)
Lehr- und Lernmethoden	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chat, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Modulverantwortliche(r)	P. Felke

Qualifikationsziele
Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage,

- ein grundlegendes Verständnis zu entwickeln in Bezug auf mögliche Angriffe auf IT-Systeme und geeignete Gegenmaßnahmen
- mögliche Schwachstellen und Bedrohungen für ein IT-System zu identifizieren
- Effektivität und Effizienz von IT-Sicherheitslösungen abzuschätzen
- Hash-Verfahren und Write-Blocker einzusetzen
- Computerforensische Spuren zu erkennen, zu sichern und auszuwerten
- forensische Hard- und Software-Tools anzuwenden
- Merkmale gerichtfester, forensischer Gutachten einzuhalten und exemplarisch anzuwenden

Lehrinhalte

Die Studierenden können einen Überblick zur Bedeutung und zu Methoden und Tools der IT-Forensik geben und erste Erfahrungen anwenden. Sie sind in der Lage Risiken einzuschätzen, Bedrohungen abzuwägen und Maßnahmen zur Sicherung von Rechnernetzen und -anwendungen zu ergreifen. Nachdem Studierende das Modul erfolgreich absolviert haben, können sie Sicherheitsprobleme in existierenden IT-Anwendungen benennen und für künftige abschätzen. Sie können Multimedia-spezifische Umsetzungen von Sicherheitsprotokollen für Bild, Video und Audio sowie weitere Mediendaten anwenden. Die Studierenden sind in der Lage, Methodik bei Entwurf und Anwendung von Sicherheitssystemen und -protokollen für Mediendaten einzusetzen. Die Studenten erwerben praktische Fähigkeiten beim Ethical Hacking durch das Lösen von Aufgaben im Hacking-Lab (www.hacking-lab.com). Lehreinheiten

1. Motivation und Einleitung
2. Ablauf von Angriffen
3. Digitale Spuren finden und deuten
4. Vorgehensmodelle & grundlegende Strategien
5. Einsatz Computerforensischer Werkzeuge
6. Beispiel praktische IT Forensik
7. Einführung und Vertiefung in die Medienforensik
8. Case Studies
9. Juristische Aspekte

Literatur

Geschonneck A.: Computer Forensik: Systemeinbrüche erkennen, ermitteln, aufklären. Dpunkt.GmbH. ISBN 3-89864-253-4. 2008 Farmer D..: Forensic discovery. Addison-Wesley. ISBN 0-201-63497-X. 2004 Carrier B.: File System Forensic Analysis. Addison Wesley Professional. ISBN 0-32-126817-2. 2005 Kent K., Chevalier S., Grance T., Dang H.: Guide to Integrating Forensic Techniques into Incident Response - NIST Special Publication 800-86. 2006 Chang-Tsun Li (Ed.): Multimedia Forensics and Security. Information Science Reference. ISBN 978-1-59904-869-7. 2009 Nelson B., Phillips A., Steuart Chr.: Guide to Computer Forensics and Investigations. Course Technolpogy ISBN 1-4354-9883-6. 2010

Lehrveranstaltungen

Dozenten/-innen	Titel der Lehrveranstaltung	SWS