Computer-Forensik (CS5329)

„Cyberkriminalität wird zum Milliardengeschäft“ - so oder ähnlich lauten Schlagzeilen in den öffentlichen Medien, die immer häufiger auf Straftaten hinweisen, bei denen IuK-Systeme und ihre Dienste als Tatmittel oder Gegenstand der strafbaren Handlung eine tragende Rolle spielen. Für die Aufklärung und Strafverfolgung solcher Delikte sind gerichtsverwertbare Beweise und die darauf basierende Rekonstruktion des Angriffs eine Grundvoraussetzung. Es ist Aufgabe der Computer-Forensik Systemeinbrüche als solche zu erkennen, digitale Spuren zu identifizieren und unter Wahrung der Integrität als Beweismittel zu sichern, mittels forensische Analyse Rückschlüsse auf den Angriffsablauf und den/die Täter zu gewinnen und schließlich die gewonnenen Daten und Erkenntnisse nachvollziehbar zu dokumentieren.

Die Lehrveranstaltung „Computer-Forensik“ behandelt alle genannten Aspekte aus theoretischer und praktischer Sicht. Sie als moderiertes Lernen organisiert. D.h., der Dozent gibt eine Einführung in die Aufgaben, Ziele und Methoden der Computer-Forensik. Unter der Moderation des Dozenten definieren und diskutieren die Teilnehmer vertiefende Themengebiete, die dann in Lerngruppen erforscht und bearbeitet werden. Die Ergebnisse werden vorgetragen.

Die Vorträge dienen als Leistungsnachweis und werden bewertet. Eine Klausur ist nicht vorgesehen.

Da die Teilnehmerzahl auf 20 begrenzt ist, ist eine Anmeldung erforderlich!

CS5329 Computer-Forensik

Studiengang	Master of Science Informatik
Modultitel	CS5329 Computer-Forensik
Dozent(in)	Schmitt, W.
Modulverantwortliche(r)	Schmitt, W.
Qualifikations- und Lernziele	*Die Kursteilnehmer kennen Aufgabenstellungen, Methoden und Werkzeuge der Computer-Forensik und sind fähig, diese in der beruflichen Praxis zu verstehen und anzuwenden.*
Lerninhalt	• *Aufgaben und Ziele und der Computer-Forensik* • *Bedrohungsszenarien und Angriffe* • *Entdeckung und Behandlung von Sicherheitsvorfällen* • *S-A-P Vorgehensmodell* • *Methoden und Werkzeuge der forensischen Analyse* • *Juristische Aspekte*
Kurzbeschreibung (ca. 20 Worte)	*Einführung in die Aufgaben, Ziele und Vorgehensweise der Computer-Forensik. Die Methoden und der Umgang mit Werkzeugen zur forensischen Analyse werden durch die Teilnehmer eigenständig erarbeitet.*
Modultyp	Wahlpflichtmodul
Moduldauer	1 Semester
Sprache	Deutsch
Lehrformen	*Moderiertes Lernen: Der Dozent gibt eine Einführung in die Aufgaben, Ziele und Methoden der Computer-Forensik. Unter der Moderation des Dozenten diskutieren und definieren die Teilnehmer vertiefende Themengebiete, die dann in Lerngruppen ausgearbeitet werden. Die Ergebnisse werden vorgetragen und bewertet.* *Umfang: 4 SWS*
Literatur	• *BSI: Leitfaden IT-Forensik* • *H. Carvey: Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7. Syngress* • *A. Geschonnek: Computer Forensik – Computerstraftaten erkennen, ermitteln, aufklären. dpunkt.verlag* • *L. Kuhlee & Victor Völzow: Computer Forensik Hacks. O'Reilly*
Creditpoints/Arbeitsaufwand	6 CrP; 180 Stunden, davon etwa 60 Stunden Präsenzzeit
Voraussetzungen	*Kenntnisse auf den Gebieten: Rechnerhardware, Betriebssysteme, Rechnernetze, IuK-Sicherkeit*
Verwendbarkeit	Master Informatik; Master Wirtschaftsinformatik; Master Medieninformatik
Voraussetzung für die Vergabe von Creditpoints / zu erbringende Leistungen	Prüfungsvorleistung: *keine* Prüfung: *Vortrag plus schriftl. Ausarbeitung*
Bewertung, Note	Bewertung der Prüfungsleistung nach § 9 der Prüfungsordnung
Häufigkeit des Angebots	jährlich

Englische Übersetzung:

Modultitel	CS5329 *Computer Forensics*
Qualifikations- und Lernziele	*Graduates know about the scope and procedures of computer forensics and are qualified to understand methods and use tools for performing computer forensic analysis.*
Lerninhalt	• *Objectives of computer-forensics* • *Threat scenarios and attacks* • *Incident detection and incident response* • *The Secure-Analyze-Present approach* • *Methods and tools for performing computer forensic analysis* • *Framing legal aspects*
Kurzbeschreibung (ca. 20 Worte)	*Introduction into the tasks, objectives and procedures of computer forensics. Acquiring independently the use of tools & methods for performing forensic analysis of IT-systems.*
Lehrformen	*Moderated approach: The lecturer introduces into the field of computer forensics by explaining tasks and objectives and outlining methods. After this, the participants discuss and define topics to be investigated within small teams. This process is moderated by the lecturer. The results elaborated will be reported by all participants and graded by the lecturer.* *Volume: 4 SWS*
Voraussetzung für die Vergabe von Creditpoints / zu erbringende Leistungen	*Prerequisites for admission to examination: none* *Examination: Oral presentation plus written composition*