Modulhandbuch zum berufsbegleitenden Bachelorstudiengang Informatik/IT-Sicherheit

Prof. Dr.-Ing. Felix C. Freiling

Friedrich-Alexander Universität
Lehrstuhl für Informatik 1

Stand: 11. November 2016

Inhaltsverzeichnis

Curriculumsübersicht **3**

Module **5**

Mathematik 1 . . . 5
Grundlagen der Programmierung . . . 8
Einführung in die IT-Sicherheit . . . 12
Konzeptionelle Modellierung . . . 15
Mathematik 2 . . . 18
Rechnerstrukturen . . . 22
Theoretische Informatik . . . 25
Systemsicherheit 1 . . . 29
Algorithmen und Datenstrukturen . . . 33
Kryptographie 1 . . . 36
Systemnahe Programmierung . . . 38
Systemsicherheit 2 . . . 41
Proseminar . . . 44
Einführung in die digitale Forensik . . . 46
Compilerbau . . . 50
Netzsicherheit 1 . . . 53
Kryptographie 2 . . . 56
Realisierung von Softwareprojekten . . . 58
Netzsicherheit 2 . . . 60
Netzsicherheit 3 . . . 63
Weiterführende Themen der Computerforensik . . . 66
Kryptographische Protokolle . . . 70
Sicherheit mobiler Systeme . . . 73
Sicherheitsmanagement . . . 76
Spam . . . 79
Netzbasierte Angriffserkennung . . . 82
User-Centered Security . . . 85
Incident Management . . . 88
Elektronische Identitäten . . . 91
Ethisches Hacking . . . 93
Anonymität im Netz . . . 97
Internetforensik . . . 101
Seminar . . . 104
Projekt . . . 106
Bachelorarbeit . . . 108

Vorwort

Dieses Dokument enthält die Beschreibungen aller Module des berufsbegleitenden Bachelorstudiengangs Informatik/IT-Sicherheit.

Die auf der Folgeseite abgebildete Curriculumsübersicht dient der allgemeinen Orientierung und der Zuordnung der Module zu den einzelnen Studiensemestern. Die Auflistung der Module in diesem Modulhandbuch entspricht im Wesentlichen dem zeitlichen Ablauf des Studiengangs.
Die in der Curriculumsübersicht grün unterlegten Module stellen die Grundlagenmodule dar, die orange unterlegten Module gehören zum allgemeinen Themenkomplex „Programmierung“, und die hellblau unterlegten Module sind dem Vertiefungsgebiet „IT-Sicherheit“ zuzuordnen. Diese drei Modulgruppen bilden zusammen die Pflichtmodule, die jeder Studierende des Studiengangs absolvieren muss. Zu den Pflichtmodulen gehören des Weiteren Proseminar, Seminar, Projekt und Bachelorarbeit.
Die dunkelblau gekennzeichneten Modulslots stehen für Wahlpflichtmodule. Insgesamt müssen aus einem Angebot von 11 Wahlpflichtmodulen 6 Module absolviert werden. Die Wahlpflichtmodule sind als weitere Vertiefung und Spezialisierung mit Schwerpunkt IT-Sicherheit anzusehen. Auf Seite 4 ist der Studienverlaufsplan dargestellt, dem insbesondere Art und Umfang der Prüfung- und Studienleistungen für die einzelnen Module zu entnehmen ist.
Dieses Modulhandbuch korrespondiert mit der Studien- und Prüfungsordnung des Studiengangs und ist Gegenstand fortgesetzter Evaluierungen.

Curriculumsübersicht

<table>
<tr><td>9</td><td rowspan="3">Wahlpflicht (6 Module aus 11 Modulen)</td><td colspan="3">Bachelorarbeit (12 ECTS) und Kolloquium (3 ECTS)</td></tr>
<tr><td>8</td><td rowspan="2">Wahlpflicht</td><td>Sicherheitsmanagement</td><td rowspan="3">Projekt (10 ECTS)
+
Seminar (5 ECTS)</td></tr>
<tr><td>7</td><td>Netzsicherheit 3</td></tr>
<tr><td>6</td><td>Realisierung von Softwareprojekten</td><td>Netzsicherheit 2</td></tr>
<tr><td>5</td><td>Einführung in die digitale Forensik</td><td>Compilerbau</td><td>Netzsicherheit 1</td><td>Kryptographie 2</td></tr>
<tr><td>4</td><td>Kryptographie 1</td><td>Systemnahe Programmierung</td><td>Systemsicherheit 2</td><td>Proseminar</td></tr>
<tr><td>3</td><td>Theoretische Informatik</td><td>Algorithmen und Datenstrukturen</td><td>Systemsicherheit 1a</td><td>Systemsicherheit 1b</td></tr>
<tr><td>2</td><td>Mathematik 2a</td><td>Programmierkonzepte</td><td>Rechnerstrukturen</td><td>Mathematik 2b</td></tr>
<tr><td>1</td><td>Mathematik 1</td><td>Einführung in das Programmieren</td><td>Einführung in die IT-Sicherheit</td><td>Konzeptionelle Modellierung</td></tr>
</table>

Studienverlaufsplan Bachelor Informatik/IT-Sicherheit

Modulbezeichnung	Lehrveranstaltung	SWS				ECTS	1.	2.	3.	4.	5.	6.	7.	8.	9.	Art und Umfang der Prüfungs- und Studienleistungen [1]
		V	Ü	P	S		ECTS	ECTS	ECTS	ECTS	ECTS	ECTS	ECTS	ECTS	ECTS	
Einführung in die IT-Sicherheit	Einführung in die IT-Sicherheit	x	x			5	5									PL (K, 60min)
Grundlagen der Programmierung	Einführung in das Programmieren	x				10	5									PL (K,120min)
	Programmierkonzepte	x	x					5								
Mathematik 1	Mathematik 1	x	x			5	5									PL (K, 60min)
Konzeptionelle Modellierung	Konzeptionelle Modellierung	x	x			5	5									PL (K, 90min)
Mathematik 2	Mathematik 2a	x	x			10		5								PL (K,120min)
	Mathematik 2b	x	x					5								
Rechnerstrukturen	Rechnerstrukturen	x	x			5		5								PL (K, 60min)
Systemsicherheit 1	Systemsicherheit 1a	x	x			10			5							PL (K,120min)
	Systemsicherheit 1b	x	x						5							
Algorithmen und Datenstrukturen	Algorithmen und Datenstrukturen	x	x			5			5							PL (K,120min)
Theoretische Informatik	Theoretische Informatik	x	x			5			5							PL (K, 60min)
Kryptographie 1	Kryptographie 1	x	x							5						PL (K, 120min)
Systemnahe Programmierung	Systemnahe Programmierung	x	x			5				5						PL (K, 120min)
Systemsicherheit 2	Systemsicherheit 2	x	x			5				5						PL (K, 60min)
Proseminar	Proseminar				x	5				5						PL (SeL)
Einführung in die digitale Forensik	Einführung in die digitale Forensik	x	x			5					5					PL (K, 60min)
Compilerbau	Compilerbau	x	x			5					5					PL (K, 120min)
Netzsicherheit 1	Netzsicherheit 1	x	x			5					5					PL (K, 120min)
Kryptographie 2	Kryptographie 2	x	x			5					5					PL (K, 120min)
Netzsicherheit 2	Netzsicherheit 2	x	x			5						5				PL (K, 120min)
Realisierung von Softwareprojekten	Realisierung von Softwareprojekten	x	x			5						5				PL (K, 60min)
Seminar	Seminar				x	5						5				PL (SeL)
Wahlpflichtbereich Unterschiedliche Module nach Wahl [2]	versch. Lehrveranstaltungen je nach Wahlmodul [2]	x	x	x		30						5	10	10	5	PL, siehe Modulhandbuch [3]
Netzsicherheit 3	Netzsicherheit 3	x	x			5							5			PL (K, 120min)
Projekt	Projekt			x		10							5	5		PfP: PL (SeL) + SL (PrL)
Sicherheitsmanagement	Sicherheitsmanagement	x	x			5								5		PL (SeL)
Bachelorarbeit	Bachelorarbeit					15									12	PL
	Kolloquium														3	
Summe SWS: 36							20	20	20	20	20	20	20	20	20	
Summe ECTS: 180																

[1] Legende zu Abkürzungen in dieser Spalte:
PL = Prüfungsleistung (benotet), SL = Studienleistung (unbenotet), PfP = Portfolioprüfung, K = Klausur mit Zeitangabe, SeL = Seminarleistung, PrL = Praktikumsleistung

[2] Für den Wahlpflichtbereich werden zur Zeit 11 Module vom Projektverbund entwickelt: Sicherheitsprotokolle, Elektronische Identitäten, Netzwerk- und Mobilfunkforensik, Modellbildung, Ethisches Hacking, Incident Management, Security Trends in Cloud Computing, Internetforensik, Implementierung kryptographischer Protokolle, Sicherheit von Webanwendungen, Sicherheit mobiler Systeme. Die Studierenden müssen 6 Module aus diesem Angebot auswählen. In Zukunft können auch weitere Module hinzukommen. Details dazu regelt das Modulhandbuch.

[3] Art und Umfang der Prüfung sind abhängig vom jeweils gewählten Modul und dem Modulhandbuch zu entnehmen.

Mathematik 1

Modulbezeichnung:	Mathematik 1
Studiengang:	Bachelor Informatik / IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Lehrveranstaltungen und Lehrformen:	Mathematik 1
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung 60 min. Um zur Prüfung zugelassen zu werden, muss die Bearbeitung, Abgabe und Vorstellung einer Übungsaufgabe in dem zur Aufgabe dazugehörigen Onlineseminar erfolgen.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Mathematik Gymnasium Oberstufe
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 1
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 30 Zeitstunden Fernstudienanteil: 120 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: • Grundlagen (Reelle und komplexe Zahlen) • Zahlentheorie und modulare Arithmetik • Vektoren und Vektorräume (Vektorrechnung im $\mathbb{R}^3$, Begriff des Vektorraums, Beispiele für Vektorräume) • Matrizen, Determinanten • Lineare Gleichungssysteme Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden können die Arithmetik reeller und komplexer Zahlen erläutern und diese anwenden. Des Weiteren kennen Sie die Grundbegriffe der Zahlentheorie sowie der modularen Arithmetik und können mit diesen umgehen, insbesondere effizient modular Potenzieren. Darüber hinaus kennen Sie das RSA-Kryptosystem und erlangen Wissen über die zugrundeliegende Sicherheit. Sie können den Begriff 'Vektorraum' erklären und können diesen auf konkrete Vektorräume anwenden. Darüber hinaus sind Sie in der Lage, mit Vektoren und Matrizen zu rechnen, insbesondere Matrizen zu invertieren. Sie kennen den Unterschied zwischen homogenen und inhomogenen linearen Gleichungssystemen und können diese systematisch lösen. *Methodenkompetenz:* Die Studierenden erwerben die Fähigkeit, mit den Lehrinhalten des Moduls aktiv umgehen zu können und können Fragestellungen, Aufgaben und Probleme, die sich aus der Lehrveranstaltung ergeben, selbstständig bearbeiten und lösen. *Sozialkompetenz:* Die Studierenden können durch Gruppenarbeit an den Präsenzwochenenden Übungsaufgaben kooperativ lösen und in Teams arbeiten. Darüber hinaus besitzen sie die Fähigkeit, in komplexen Situationen zu handeln und Lösungen für Aufgabenstellungen zu entwickeln. *Selbstkompetenz:* Die Studierenden können aufgrund der Teamarbeit problemorientiert diskutieren. Sie haben die Fähigkeit, sich eine Meinung über die Themen von Mathematik 1 zu bilden und können das erlangte Wissen im Bereich der Informatik einsetzen.
Häufigkeit des Angebots:	Wintersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Teschl, G.; Teschl, S.: Mathematik für Informatiker Band 1: Diskrete Mathematik und Lineare Algebra, Springer-Verlag, ISBN 978-3-642-37972-7, Springer; Auflage: 4 • Teschl, G.; Teschl, S.: Mathematik für Informatiker Band 2: Analysis und Statistik, Springer-Verlag, ISBN 978-3-642-54274-9, Springer; Auflage: 3 • Arens, T.; Hettlich, F.; Karpfinger, C.; Kockelkorn, U.; Lichtenegger, K.; Stachel, H.: Mathematik, Springer-Verlag, ISBN: 978-3-827-42347-4, Springer; Auflage: 2 • Arens, T.; Hettlich, F.; Karpfinger, C.; Kockelkorn, U.; Lichtenegger, K.; Stachel, H.: Arbeitsbuch Mathematik - Aufgaben, Hinweise, Lösungen und Lösungswege, Springer-Verlag, ISBN: 978-3-827-42410-5, Springer; • Arens, T.; Busam, F.; Hettlich, F.; Karpfinger, C.; Stachel, H.; Lichtenegger, K.: Grundwissen Mathematikstudium - Analysis und Lineare Algebra mit Querverbindungen, Springer-Verlag, ISBN: 978-3-827-42309-2, Springer;

Grundlagen der Programmierung

Modulbezeichnung:	Grundlagen der Programmierung
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Einführung in das Programmieren Programmierkonzepte
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Prof. Dr. Felix Freiling
Dauer:	2 Semester
Credits:	10 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 Minuten Um zur Prüfung zugelassen zu werden, müssen die bereitgestellten Übungsaufgaben in jeder Lehrveranstaltung zu mindestens 70% richtig bearbeitet werden.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Keine
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 1
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz

Arbeitsaufwand bzw. Gesamtworkload:	Für dieses Modul: Präsenzzeit: 60 h • Vorlesungsteil: 20 h • Übungsteil: 10 h • Praktischer Teil: 20 h • Prüfungsvorbereitungsveranstaltung: 8 h • Prüfung: 2 h Eigenstudium: 240 h • Durcharbeiten der Studienbriefe: 100 h • Wahrnehmen der Online Betreuung und Beratung: 20 h • Ausarbeiten von Aufgaben: 100 h • Individuelle Prüfungsvorbereitung der Studierenden: 20 h

Lerninhalt und Niveau:	**Einführung in das Programmieren** Eine Einführung in die Programmiersprache Java. Mit Hilfe der Entwicklungsumgebung BlueJ wird den Studierenden der Umgang mit Java und Objektorientierung vertraut gemacht. Themen sind unter anderem: • Ausdrücke und Algorithmische Kernsprache von Java • Sprachbeschreibung und Objekttypen • Eine Einführung in bereits existierende Methoden und Klassen in der Programmiersprache Java • Polymorphie und Generics • Testen und Test Driven Development mit JUnit Darüber hinaus erhalten die Studierenden einen praktischen Einblick in die folgenden programmierrelevanten Technologien/Techniken: • Versionsverwaltung mit Git **Programmierkonzepte** Diese Lehrveranstaltung knüpft nahtlos an die Veranstaltung „Einführung in das Programmieren“ an. Die Studierenden lernen weitere Komponenten der Programmiersprache Java kennen, wie beispielsweise: • Exceptionhandling • I/O-Verarbeitung • Rekursion • Komplexität und Verifikation von Algorithmen Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden können beliebige Programme in Java erstellen. Sprachkomponenten, die Sie noch nicht kennen, können Sie sich in kürzester Zeit aneignen. Zudem sind die Studierenden in der Lage, sich selbstständig neue Programmiersprachen beizubringen. Sie schreiben sichere Programme und wissen, wo potenzielle Schwachstellen in einem Programm zu finden sind. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit beliebigen IDEs. Sie können fremde Programme untersuchen und den Kontrollfluss nachvollziehen. Sie sind in der Lage, Schwachstellen und Fehler in einem Programm zu finden und zu beseitigen. *Sozialkompetenz:* Durch das gemeinsame Lösen von Aufgaben erlangen die Studierenden die Fähigkeit, eigene Handlungsziele mit den Einstellungen und Werten einer Gruppe zu verknüpfen und ihre Teamfähigkeit zu stärken. In der Präsenzphase erlangen sie u. a. durch Pair-Programming die Kompetenz, eigene Ideen gegenüber einem anderen Programmierer zu kommunizieren, Kompromisse zu bilden und diese im Team umzusetzen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über eigene Programme und Programme anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Häufigkeit des Angebots:	Wintersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	• IT-Sicherheit, Claudia Eckert, 2012 • Java lernen mit BlueJ, David J. Barnes, Michael Kölling, 2013 • Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Einführung in die IT-Sicherheit

Modulbezeichnung:	Einführung in die IT-Sicherheit
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Einführung in die IT-Sicherheit
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 1
Generelle Zielsetzung des Moduls:	Modul zur Einführung in das Basiswissen der IT-Sicherheit
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • davon Selbststudium: 105 Zeitstunden • davon Aufgaben: 20 Zeitstunden • davon Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalt und Niveau:	Auf folgende Themengebiete wird eingegangen: • Grundlagen des Sicherheitsmanagements, des Risikomanagements und der -analyse • Notfallplanung • Bedrohungsfaktoren der IT-Sicherheit und deren Schutzmaßnahmen • Grundlagen der Zugriffskontrolle und -verwaltung • Mechanismen der Authentisierung, SSO-Technologien • Darstellung der Angriffe auf Zugriffskontrollsysteme • Einführung in die Kryptographie, symmetrische und asymmetrische Verschlüsselungsverfahren, Darstellung der Angriffe auf Kryptosysteme, kryptographische Hashfunktionen, digitale Signatur • Einführung in die Steganographie • Einführung in die Sicherheitsaspekte vernetzter Umgebungen, Grundlagen des DNS, E-Mail-Missbrauch • Spam, Phishing, Network Security Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden haben Grundkenntnisse des Sicherheitsmanagements, des Risikomanagements und der -analyse. Die Studierenden haben sich Grundlagen der Zugriffskontrolle und -verwaltung angeeignet, können Mechanismen der Authentisierung unterscheiden und erklären sowie SSO-Technologien beschreiben. Sie sind in der Lage, die unterschiedlichen Angriffe auf Zugriffskontrollsysteme darzustellen. Sie haben Grundkenntnisse der Kryptographie und Steganographie, können symmetrische und asymmetrische Verschlüsselungsverfahren differenzieren, Angriffe auf Kryptosysteme darstellen sowie kryptographische Hashfunktionen und digitale Signatur erklären. Zudem sind die Studierenden mittels ihrer Grundkenntnisse über die Sicherheitsaspekte vernetzter Umgebungen und das DNS in der Lage, diese zu erläutern. Sie können einen E-Mail-Missbrauch und Spam erklären sowie Phishing aufzeigen und ihre Lösungsansätze darstellen. *Methodenkompetenz:* Die Studierenden können eine Notfallplanung erläutern, die Bedrohungsfaktoren der IT-Sicherheit beschreiben und klassifizieren sowie deren Schutzmaßnahmen skizzieren und anwenden. Der Lernende kann die Phasen eines Hackerangriffs strukturieren, Malware analysieren und einordnen und die entsprechenden Schutzmaßnahmen anwenden. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen. *Selbstkompetenz:* Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.
Häufigkeit des Angebots:	in jedem Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literatur:	• Sicherheit in Informationssystemen, (Vorlesungsskript), Daniel Hammer, 2012 • Angewandte Kryptographie, Bruce Schneier, 1996 • Netzsicherheit, Günter Schäfer, 2003 • Cyberwar: Das Internet als Kriegsschauplatz, Sandro Gaycken, 2011 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Konzeptionelle Modellierung

Modulbezeichnung:	Konzeptionelle Modellierung
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Konzeptionelle Modellierung
Modulverantwortliche(r):	Prof. Dr. Richard Lenz
Lehrende:	Prof. Dr. Richard Lenz/Prof. Dr. Felix Freiling
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 90 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	Keine
Empfohlene Voraussetzungen:	Keine
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 1
Generelle Zielsetzung des Moduls:	Zur Förderung und Verstärkung der Fachkompetenz

Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 30 h • Vorlesungsteil: 10 h • Übungsteil: 5 h • Praktischer Teil: 10 h • Prüfungsvorbereitungsveranstaltung: 4 h • Prüfung: 1 h Eigenstudium: 120 h • Durcharbeiten der Studienbriefe: 50 h • Durcharbeiten des Online-Lernmaterials: 10 h • Wahrnehmen der Online-Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 20 h
Lerninhalt und Niveau:	Im Modul konzeptionelle Modellierung wird auf folgende Themengebiete eingegangen: • Grundlagen der Modellierung • Entity-Relationship Modell (ER-Modell) • Metamodellierung und XML • Datenmodellierung und Domänenmodellierung Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die Grundlagen der Modellierung sowie über das Entity-Relationship-Modell (ER-Modell). Darüber hinaus erwerben Sie fundiertes Wissen über die Datenbanksprache SQL sowie die Auszeichnungssprache XML. *Methodenkompetenz:* Die Studierenden haben die Fähigkeit zu beurteilen, wann eine Datenbank sinnvoll ist und können zwischen verschiedenen Typen von Datenbanksystemen unterscheiden. *Sozialkompetenz:* Die Konflikt- und Kommunikationsfähigkeit der Studierenden wird in den gemeinsamen Online-Tutorien und Diskussionsforen geschult. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die selbstentwickelten Datenmodellierungen und die Datenmodellierungen anderer. Darüber hinaus erlangen sie die Fähigkeit, in herausfordernden Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.

Häufigkeit des Angebots:	Wintersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer.
Literatur:	• Konzeptionelle Modellierung, Richard Lenz, 2012 • Datenbanksysteme: Eine Einführung, Alfons Kemper und Andre Eickler • An Introduction to Database Systems, C. J. Date • Analyse und Design mit UML 2.1, B. Oestereich • XML und Datenmodellierung, R. Eckstein und S. Eckstein • XML und Datenbanken, H. Schoening • XML Tutorial, Refsnes Data • Extensible Markup Language (XML), Mario Jeckle • Date Warehouse Systems, Andreas Bauer und Holger Guenzel • Information Modeling and Relational Database, T. Halpin und T-Morgan • Mehrrechner- Datenbanksysteme, E. Rahm • Lehrbuch der Softwaretechnik, H. Bazert • Datenbankmodelle, Datenbanksprachen und Datenbankmanagementsysteme, G. Vossen • Datenbanken – Konzepte und Sprachen, G. Saake, K. Sattler und A. Heuer • Duden 01. Die deutsche Rechtschreibung: Das umfassende Standardwerk auf der Grundlage der aktuellen amtlichen Regeln, Dudenverlag • Grundlagen der Informatik, Helmut Herold und Bruno Lurz und Jürgen Wohlrab • Relationale Datenbanken, Hermann Sauer

Mathematik 2

Modulbezeichnung:	Mathematik 2
Studiengang:	Bachelor Informatik / IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Lehrveranstaltungen und Lehrformen:	Mathematik 2a und 2b
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	10 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung 120 min. (Mathematik 2a und 2b) Um zur Prüfung zugelassen zu werden, muss die Bearbeitung, Abgabe und Vorstellung einer Übungsaufgabe in dem zur Aufgabe dazugehörigen Onlineseminar erfolgen.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Mathematik 1
Empfohlene Voraussetzungen:	keine
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 2
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 60 Zeitstunden Fernstudienanteil: 240 Zeitstunden • Selbststudium: 180 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 20 Zeitstunden **Summe: 300 Zeitstunden**

Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: • Mathematik 2a: – Folgen und Funktionen (Konvergenz von Folgen und Reihen, Stetigkeit von Funktionen) – Differentialrechnung einer und mehreren Veränderlichen – Partielle Ableitungen • Mathematik 2b: – Integralrechnung einer und mehreren Veränderlichen – Numerik (Rechnerarithmetik, Algorithmen, Lineare Gleichungssysteme, Interpolation, Approximation, Numerische Integration, Numerische Differentiation) – Kombinatorik und endliche Wahrscheinlichkeitstheorie (Elementare Zählprobleme, Binominialkoeffizient und Teilmengen, Permutation, Partitionen, Grundbegriffe der endlichen Wahrscheinlichkeitstheorie, bedingte Wahrscheinlichkeiten, Zufallsgrößen) – Wahrscheinlichkeitsrechnung (ausgewählte diskrete Verteilungen, Normalverteilung, Testverteilung) Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Mathematik 2a: Die Studierenden können entscheiden, ob Folgen bzw. Reihen konvergent sind oder nicht und ggf. Grenzwerte berechnen. Des Weiteren können Sie die elementaren Funktionen der Analysis erläutern und haben Kenntnisse über ihre grundlegenden Eigenschaften. Sie verstehen die Integral- und Differentialrechnung und können diese anwenden. Des Weitern kennen Sie die Grundbegriffe der Zahlentheorie, sowie der modularen Arithmetik und können mit diesen umgehen. Mathematik 2b: Die Studierenden verstehen die Integralrechnung und können diese anwenden. Sie wissen, wie Computersysteme Zahlen darstellen und können die Laufzeit eines Algorithmus berechnen. Sie kennen die Begriffe Interpolation, Approximation, numerische Integration und Differentiation. Weiter kennen Sie die elementaren Zählprobleme und können mit Hilfe des Binominialkoeffizienten die Anzahl von Möglichkeiten berechnen. Am Ende kennen Sie die Grundbegriffe der endlichen Wahrscheinlichkeitstheorie und können mit den Begriffen bedingte Wahrscheinlichkeiten und Zufallsgrößen umgehen. Darüber hinaus kennen Sie ausgewählte diskrete Verteilungen, Normalverteilung, Testverteilung und können damit umgehen. *Methodenkompetenz:* Die Studierenden können mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen die fachgebundene Diskussion, die sich aus der gemeinsamen Teamarbeit zum Lösen von Aufgaben ergeben. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Themen von Mathematik 2 zu bilden und besitzen darüber hinaus die Kompetenz Sie in den entsprechenden Gebieten der Informatik einsetzen zu können.
Häufigkeit des Angebots:	Sommersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Teschl, G.; Teschl, S.: Mathematik für Informatiker Band 1: Diskrete Mathematik und Lineare Algebra, Springer-Verlag, ISBN 978-3-642-37972-7, Springer; Auflage: 4 • Teschl, G.; Teschl, S.: Mathematik für Informatiker Band 2: Analysis und Statistik, Springer-Verlag, ISBN 978-3-642-54274-9, Springer; Auflage: 3 • Knorrenschild, M.: Numerische Mathematik - Eine beispielorientierte Einführung, Fachbuchverlag Leipzig, ISBN: 978-3-446-43233-8, Auflage: 5 • Arens, T.; Hettlich, F.; Karpfinger, C.; Kockelkorn, U.; Lichtenegger, K.; Stachel, H.: Mathematik, Springer-Verlag, ISBN: 978-3-8274-2347-4, Springer; Auflage: 2 • Arens, T.; Hettlich, F.; Karpfinger, C.; Kockelkorn, U.; Lichtenegger, K.; Stachel, H.: Arbeitsbuch Mathematik - Aufgaben, Hinweise, Lösungen und Lösungswege, Springer-Verlag, ISBN: 978-3-827-42410-5, Springer; • Arens, T.; Busam, F.; Hettlich, F.; Karpfinger, C.; Stachel, H.; Lichtenegger, K.: Grundwissen Mathematikstudium - Analysis und Lineare Algebra mit Querverbindungen, Springer-Verlag, ISBN: 978-3-827-42309-2, Springer;

Rechnerstrukturen

Modulbezeichnung:	Rechnerstrukturen
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Rechnerstrukturen
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	Einführung in die IT-Sicherheit
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 2
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalt und Niveau:	Im Modul Rechnerstrukturen wird auf folgende Themengebiete eingegangen: • Darstellung von Daten in einer computergerechten Weise • Schaltalgebra • Wichtige Rechnerstrukturen, einschließlich Prozessoren, Peripheriegeräten, Speicherorganisation und Verbindungsstrukturen • Maschinenorientierte Programmiersprachen Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben Grundkenntnisse über die computergerechte Darstellung von Daten. Ferner eignen Sie sich Grundlagen der Schaltalgebra an und können Schaltnetze bzw -werke beschreiben und klassifizieren. *Methodenkompetenz:* Die Studierenden erlangen das Grundwissen über Rechnerarchitektur und können den Aufbau und die Komponenten verschiedener Rechnerarchitekturen darstellen und z. B. das Prinzip des Universalrechners erläutern und Prozessoren, Peripheriegeräte und Speicherorganisation erklären. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können den Aufbau und die Funktionsweise von Rechnern verstehen und nachvollziehen. Desweiteren verfügen sie nach Absolvieren des Moduls über Kenntnisse der verschiedenen Abstraktionsebenen von Computern und deren Zusammenwirken. Ihnen wird bewusst, dass IT sehr schnelllebig ist und dass Detailwissen eine kurze Halbwertzeit hat. Sie sind in der Lage sich je nach Bedarf selbst weiterzubilden. Nach Bearbeitung diese Moduls verstehen die Studierenden den Computer als System und haben die grundlegenden Prinzipien verinnerlicht.
Häufigkeit des Angebots:	in jedem Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	• Rechnerarchitektur & Betriebssysteme, (Vorlesungsskript), Daniel Hammer, 2012 • Rechneraufbau und Rechnerstrukturen, W. Oberschelp, G.Vossen, 2003 • Computerarchitektur, Andrew S. Tanenbaum, 2005 • Einführung in die Rechnerarchitektur, Christian. Märtin, Leipzig, 2003 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Theoretische Informatik

Modulbezeichnung:	Theoretische Informatik
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Theoretische Informatik
Modulverantwortliche(r):	Prof. Dr. Marian Margraf
Lehrende:	Prof. Dr. Marian Margraf
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Mathematik 2
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 3
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz

Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150h Präsenzanteil: 30h • Vorlesungsteil: 12h • Virtuelle Lehre: 10h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 5h • Prüfung: 1h Fernstudienanteil: 120h • Durcharbeiten der Studienbriefe: 70h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 20h • Individuelle Prüfungsvorbereitung der Studierenden: 20h
Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: • Grundbegriffe: Wörter, Alphabete, Relationen, Operationen über Relationen • Formale Sprachen/Automatentheorie: Chomsky Grammatiken, Chomsky Hierarchie, Wortproblem, Reguläre Sprachen, deterministische und nichtdeterministische Automaten, Minimierungsalgorithmus für deterministische Automaten, Kontextfreie Sprachen, CYK-Algorithmus • Berechnungstheorie: Berechenbarkeitsmodelle (RAM und TuringMaschinen), Churchsche These, Unentscheidbarkeit und TuringReduzierbarkeit • Komplexitätstheorie: nichtdeterministische Turing-Maschinen, Komplexitätsmaße, Komplexitätsklassen, linear beschränkte Automaten und kontext-sensitive Sprachen, das P=NP? Problem, polynomielle Reduzierbarkeit, NP-Vollständigkeit Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erlangen ein Verständnis für grundlegende Konzepte, Begriffe und Zusammenhänge aus den Teilgebieten Automatentheorie, formale Sprachen, Berechnungstheorie und P/NP-Theorie und haben ein Verständnis für grundlegende Beweismethoden entwickelt. Sie haben die Fähigkeit herausbildet, einfache Beweise selbständig zu führen. Des Weiter haben Sie Kenntnis von der Leistungsfähigkeit unterschiedlicher Beschreibungsmittel und haben die Fähigkeit entwickelt, die Beschreibungsmittel selbständig zu gebrauchen. Darüber hinaus haben Sie das Wissen um den Zusammenhang zwischen der Leistungsfähigkeit und der algorithmischen Beherrschbarkeit unterschiedlicher Beschreibungsmittel erlangt. Die Studierenden haben weiter ein Verständnis für nichtdeterministische Maschinenmodelle und deren Bedeutung entwickelt. Sie können mit den deterministischen und nichtdeterministischen Maschinenmodellen umgehen und haben ein Verständnis für die algorithmische Lösbarkeit/Nichtlösbarkeit von Problemen sowie die inhärente Komplexität von Problemen entwickelt. *Methodenkompetenz:* Die Studierenden können Fragen zu den oben genannten Fachkompetenzen schriftlich beantworten. Sie können zu gegebenen formalen Sprachen Grammatiken und Automaten entwickeln, welche die gegebene formale Sprache erzeugt und akzeptiert. Darüber hinaus können Sie die Korrektheit ihrer Entwicklung zeigen. Sie können einen gegebenen deterministischen Automaten minimieren und gegebene kontextfreie Grammatiken in die Chomsky-Normalform umwandeln. Weiter können Sie zeigen, ob eine einfache Sprache regulär ist oder nicht und für die Sprache erläutern, zu welcher Klasse von Sprachen sie gehört. Sie beherrschen die grundlegenden Beweismethoden und haben die Fähigkeit, einfache Beweise selbständig zu führen. Sie können einfache Programme bei den unterschiedlichen Berechenbarkeitsmodelle formulieren, ihre Korrektheit beweisen und zeigen ob eine vorgegebene Menge entscheidbar/unentscheidbar ist. Sie können weiter zeigen, ob eine gegebene Menge NP-vollständig ist. *Sozialkompetenz:* Die Studierenden sind in der Lage als Team zusammenzuarbeiten und so Lösungen für die gestellten Aufgaben zu finden. Darüber hinaus können Sie zu den Themen eine fachgebundene Diskussion führen. *Selbstkompetenz:* Die Studierenden sind in der Lage die Lösungen zu den Aufgaben und Problemen mündlich und schriftlich zu formulieren und zu präsentieren. Dadurch könne Sie sich auch gegen Einwände in einer Diskussion verteidigen. Sie sind in der Lage selbständig geeignete Literatur zu finden und einzusetzen.
Häufigkeit des Angebots:	Sommersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	

Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: 1. Eigenes Skript 2. Hromkovic, J.: Theoretische Informatik, Teubner Verlag, Stuttgart, 2002. 3. Schöning, U.: Theoretische Informatik – kurz gefaßt, Spektrum Akademischer Verlag, Heidelberg, 1997. 4. I. Wegener, I.: Theoretische Informatik – eine algorithmenorientierte Einführung, Teubner Verlag, Stuttgart, 1999. 5. Wegener, I: Komplexitätstheorie: Grenzen der Effizienz von Algorithmen (Springer-Lehrbuch) (German Edition); Auflage: 2003 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Systemsicherheit 1

Modulbezeichnung:	Systemsicherheit 1
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Systemsicherheit 1a und 1b
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	10 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 3
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 30 Zeitstunden Fernstudienanteil: 270 Zeitstunden • Selbststudium: 210 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 20 Zeitstunden Summe: 300 Zeitstunden

Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: Systemsicherheit 1a: • Eine Einführung in die Grundlagen von Betriebssystemen, ihre Aufgaben und Ausprägungen • Prozesse, Threads, Prozessmodell und Prozesssteuerung • Synchronisation, Context Switch • Deadlocks Systemsicherheit 1b: • Grundwissen über Dateisysteme • Grundlagen der Speicherverwaltung und virtuelle Speicher • Basiswissen über Scheduling • Ein- und Ausgabe Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Systemsicherheit 1a: Die Studierenden erwerben Grundkenntnisse über Betriebssysteme, ferner eignen sie sich Grundlagen der Prozessorganisation an, können Prozesse und Threads erklären, das Prozessmodell und die Prozesssteuerung beschreiben und Synchronisation und Context Switch erläutern. Außerdem erwerben sie Grundkenntnisse über Deadlocks. Systemsicherheit 1b: Die Studierenden erlangen anhand von UNIX-Beispielen das Basiswissen über Dateisysteme und sie erwerben Kenntnisse über den Aufbau eines Dateisystems. Ferner eignen sie sich Grundlagen der Speicherverwaltung an. Außerdem erhalten sie das Basiswissen über Scheduling und die Ein- und Ausgabe. *Methodenkompetenz:* Die Studierenden kennen unterschiedliche Arten von Betriebssystemen und können sie differenzieren und wissen außerdem wie ein ausführbares Programm entsteht. Sie sind in der Lage zwischen Prozessen und Threads zu unterscheiden und das Prozessmodell, die Prozesssteuerung und Context Switch zu erläutern. Die Lernenden können anhand der erlernten Lösungsansätze einen wechselseitigen Ausschluss lösen. Sie sind nach Durcharbeiten dieses Moduls in der Lage eigenständig Deadlocks zu modellieren und sie können Deadlock-Behandlungsstrategien anwenden. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Häufigkeit des Angebots:	in jedem Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	• Rechnerarchitektur & Betriebssysteme, (Vorlesungsskript), Daniel Hammer, 2012 • Betriebssysteme, Eduard Glatz, 2005 • Moderne Betriebssysteme, Andrew S. Tanenbaum, 2003 • Betriebssysteme - Prinzipien und Umsetzung, William Stallings, 2005 • Netzsicherheit, Günter Schäfer, 2003 • Computer Security, Dieter Gollmann, 2010 • Security Engineering - A guide to Building - Dependable Distributed Systems, Ross Anderson, 2010 • Deadline Scheduling for Real-Time Systems, John A. Stankovic, 1998 • Fundamentals of Operating Systems, R.D.Eager, A.M.Lister, 1993 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Algorithmen und Datenstrukturen

Modulbezeichnung:	Algorithmen und Datenstrukturen
Studiengang:	Bachelor Informatik/IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Algorithmen und Datenstrukturen
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Dr. Werner Massonne
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module, insbesondere • Programmierkonzepte • Mathematik 1
Empfohlene Voraussetzungen:	Erfolgreicher Abschluss der Module • Mathematik 2 (Wahrscheinlichkeitsrechnung aus Lehrveranstaltung Mathematik 2b)
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 3
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: • Programmierkurs zur Erlernung der Programmierung in C • Analysemodell, Lauzeitmodelle und allgemeine Analysetechniken für Algorithmen • Strukturierte Datentypen wie Arrays, Listen, Bäume und Graphen • Verschiedene Sortieralgorithmen mit ihren Laufzeitanalysen • Algorithmen auf Mengen: Suchen, TRIES, Hashing, Union-Find und Priority Queues • Balancierte Suchbäume, insbesondere AVL-Bäume und B-Bäume • Repräsentation von Graphen und fundamentale Algorithmen auf Graphen • Vertiefung der Graphenalgorithmen: Zusammenhangskomponenten und Bestimmung kürzester Pfade • Implementierung der vorgestellten Algorithmen in C **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)**
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse in der Programmiersprache C. Sie lernen grundlegende Datenstrukturen und Algorithmen der Informatik kennen und erlernen, diese bezüglich Effizienz einzuschätzen und in einer konkreten Programmiersprache umzusetzen. *Methodenkompetenz:* Die Studierenden erwerben die Fähigkeit, konkrete Programmieraufgaben in einer höheren Programmiersprache zu formulieren. Lernende können hierbei die Gesamtaufgabe strukturieren und in Teilaufgaben zerlegen. Die Studierenden erlernen die Fähigkeit, geeignete Datenstrukturen und Algorithmen zur Abbildung von Programmieraufgaben zu finden, die eine effiziente Umsetzung gestatten. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die eigenen Programme und die Programme anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Häufigkeit des Angebots:	Wintersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	

Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Programmieren in C, Kernighan und Ritchie, 1990 • Algorithmen – kurz gefasst, Uwe Schöning, 1997 • Algorithms and Data Structures: The Basic Toolbox, Mehlhorn and Sanders, 2010 • Algorithmen - Eine Einführung, Corman, Leiserson, Rivest und Stein, 2010 • Datenstrukturen und Effiziente Algorithmen, Band 1: Sortieren und Suchen, Kurt Mehlhorn, 1986 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Kryptographie 1

Modulbezeichnung:	Kryptographie 1
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Kryptographie 1
Modulverantwortliche(r):	Prof. Dr. Christof Paar
Lehrende:	Prof. Dr. Christof Paar
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch, Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 4
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h

Lerninhalt und Niveau:	In diesem Modul werden zunächst einige grundlegende Begriffe der Datensicherheit erläutert. Danach werden einige historisch wichtige Verschlüsselungsverfahren vorgestellt. Die Schwerpunkte dieses Moduls liegen auf der Besprechung von praktisch wichtigen Verschlüsselungsverfahren, Hashfunktionen und Message Authentication Codes (MAC). Als bedeutende Vertreter der symmetrischen Verfahren werden der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES) behandelt. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die Bedeutung von symmetrischen kryptographischen Verfahren und verstehen die Strukturen der prominentesten symmetrischen Primitiven. Darüber hinaus verinnerlichen die Studenten die Sicherheitskonzepte und diverse Angriffsziele von symmetrischen Verfahren. Die Grundprinzipien asymmetrischer Kryptographie werden verstanden. *Methodenkompetenz:* Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von symmetrischen Verfahren nachvollziehen. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen von symmetrischen kryptographischen Verfahren aus und diskutieren Lösungswege von Problemen. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit aktuelle symmetrische kryptographische Verfahren zu verstehen und eine fundierte Meinung über die Sicherheit dieser Verfahren zu vertreten. Darüber hinaus besitzen die Studierenden alle Voraussetzungen neue symmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen einzuschätzen.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Handbook of Applied Cryptography, Alfred J. Menezes, Paul C van Oorschot, Scott A Vanstone, 1996 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Systemnahe Programmierung

Modulbezeichnung:	Systemnahe Programmierung
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Systemnahe Programmierung
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Dr. Werner Massonne
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module, insbesondere: • Algorithmen und Datenstrukturen • Rechnerstrukturen
Empfohlene Voraussetzungen:	Erfolgreicher Abschluss der Module • Systemsicherheit 1a und 1b
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 4
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: • Allgemeine Rechner- und Betriebssystemstrukturen • Innere Strukturen des Betriebssystems Microsoft Windows • Assemblerprogrammierung der Intel-Architektur-32 (IA-32) • Codeerzeugung, Codeoptimierung und Programmanalyse für IA-32 • Systemnahe Sicherheitsaspekte, insbesondere Mechanismen von Buffer Overflow und sonstigen Sicherheitslücken sowie Gegenmaßnahmen zur Verhinderung ihrer Ausbeutung • Obfuscation und sonstige Malware-Techniken. Malware-Analyse durch das Analyseprogramm IDA anhand realer Beispiele **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden haben fundierte Kenntnisse in der Programmierung von IA-32 auf Maschinenebene. Sie können Maschinencode aus der Hochsprache C erzeugen und haben einen Überblick über Verfahren zur Codeoptimierung und Codeverschleierung (Obfuscation). Die Studierenden haben einen Einblick in die Funktionsweise von Malware auf Systemebene und können einfache Malware selbstständig analysieren. *Methodenkompetenz:* Die Studierenden haben die Fähigkeit, systemnahe Programme zu erstellen und zu verstehen. Die Studierenden können Probleme auf dieser Ebene der Programmierung erkennen und Schwachstellen identifizieren und analysieren. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Durch das eigenverantwortliche Entwickeln von Programmen erweitern die Studierenden ihr selbstständiges Handeln. Durch die Präsentation ihrer Ergebnisse wird die Selbstsicherheit der Studierenden gestärkt.
Häufigkeit des Angebots:	Sommersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Intel 80386, Programmers Reference Manual, 1987 • Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Sikorski and Honig, 2012 • Reversing: Secrets of Reverse Engineering, Eilam, 2005 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Systemsicherheit 2

Modulbezeichnung:	Systemsicherheit 2
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Systemsicherheit 2
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	Systemsicherheit 1a/1b
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 4
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalt und Niveau:	Im Modul Systemsicherheit 2 wird auf folgende Themengebiete eingegangen: • Malware • Sicherheitsmechanismen- und modelle • Vorstellung und Erläuterung der Sicherheitsaspekte von Betriebssystemen. • Angriffsszenarien • Abwehrmechanismen Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erlangen anhand von Beispielen das Basiswissen über Malware, wie diese Schadsoftware funktioniert und welche Gefahr von ihr ausgeht. Ferner erwerben sie Kenntnisse über die Sicherheitsmechanismen und -modelle von Betriebssystemen und können zwischen unterschiedlichen Angriffsszenarien differenzieren. Außerdem eignen sie sich das Wissen über die entsprechenden Abwehrmechanismen an. *Methodenkompetenz:* Die Studierenden können zwischen den unterschiedlichen Malware-Arten differenzieren und können die entsprechenden Schutzmaßnahmen einsetzen. Sie kennen die Sicherheitsmechanismen- und modelle von Betriebssystemen und ihre unterschiedlichen Sicherheitsaspekte. Außerdem wissen die Studierenden wie Programmierfehler ausgenutzt werden können, was Insider-Angriffe sind und wie und welche Abwehrmechanismen sie einsetzen können. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Häufigkeit des Angebots:	in jedem Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	• IT-Sicherheit: Konzepte - Verfahren - Protokolle, Claudia Eckert, 2006 • Moderne Betriebssysteme, Andrew S. Tanenbaum, 2003 • Betriebssysteme - Prinzipien und Umsetzung, William Stallings, 2005 • Malware, Eugene Kaspersky, 2008 • Computer Security, Dieter Gollmann, 2010 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Proseminar

Modulbezeichnung:	Proseminar
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	berufsbegleitender Bachelorstudiengang IT-Sicherheit
Lehrveranstaltungen und Lehrformen:	Proseminar
Modulverantwortliche(r):	Betreuender Dozent kann jeder Professor oder Lehrbeauftragter des Studiengangs sein.
Lehrende:	Betreuender Dozent kann jeder Professor oder Lehrbeauftragter des Studiengangs sein.
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Ausarbeitung im Umfang von 5-15 Seiten, mündliche Präsentation im Umfang von 45 Minuten
Berechnung der Modulnote:	
Notwendige Voraussetzungen:	Keine
Empfohlene Voraussetzungen:	Keine
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Studiensemester 4
Generelle Zielsetzung des Moduls:	
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 1 h • Seminarvortrag: Präsentation und Diskussion Eigenstudium: 149 h • Themenbearbeitung • Besprechungen mit dem Betreuer • Vorbereitung der Präsentation
Lerninhalt und Niveau:	Der Themenbereich des Proseminars wird vor Semesterbeginn bekanntgeben. Jeder Studierende erhält ein individuelles, begrenztes Thema (z.B. Buchkapitel oder Konferenzveröffentlichung). Dieses wird nach den Kriterien wissenschaftlichen Arbeitens schriftlich ausgearbeitet und mündlich vor den Mitstudenten und Betreuern präsentiert. Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erkennen die Wichtigkeit des exakten wissenschaftlichen Arbeitens. Sie können eine begrenzte Fragestellung auf dem Gebiet der Informatik selbstständig recherchieren und ihre Ergebnisse präsentieren und verteidigen. *Methodenkompetenz:* Die Studierenden erkennen die Wichtigkeit des methodischen Arbeitens im wissenschaftlichen Umfeld und können diese Methodik bei einem begrenzten, vorgegebenen Thema anwenden. *Sozialkompetenz:* Durch die enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können fachbezogene Inhalte klar und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten.
Häufigkeit des Angebots:	Sommersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	
Literatur:	

Einführung in die digitale Forensik

Modulbezeichnung:	Einführung in die digitale Forensik
Studiengang:	Bachelor Informatik / IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Lehrveranstaltungen und Lehrformen:	Einführung in die digitale Forensik
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss des Moduls • System Sicherheit 1a
Empfohlene Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Einführung IT Sicherheit
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 5
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 30 Zeitstunden Fernstudienanteil: 120 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: • Klassische forensische Wissenschaften und digitale Forensik. • Grundlagen der digitalen Forensik. • Digitale Spuren (Entstehung, Manipulier- und Kopierbarkeit, Personenbezogenheit). • Einführung in die Dateisystemanalyse (Generelles Konzept, FAT, NTFS). • Analyse mit forensischen Tools (Sleuthkit, Autopsy, DFF, Filecarver). • Vorgehensmodelle und Gutachtenerstellung. • Einführung in die Hauptspeicherforensik anhand. • Hashfunktionen in der digitalen Forensik. • Praktische Bearbeitung von Aufgaben Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die Grundlagen der digitalen Forensik und können diese anwenden. Sie haben Kenntnis über die Entstehung, der Manipulier- und Kopierbarkeit sowie der Personenbezogenheit von digitalen Spuren. Sie kennen weiter das grundlegende Konzept sowie die Eigenschaften der gängigen Dateisysteme FAT und NTFS und können mit diesem Wissen eine Dateisystemanalyse durchführen. Darüber hinaus kennen Sie die grundlegenden Schritte eines IT-Forensikers und können mit allgemeinen und speziellen forensischen Werkzeugen sicher umgehen. Des Weiteren sind die Studierenden mit der grundlegenden Funktionsweise kryptographischer Hashfunktionen, sowie deren Rolle in der digitalen Forensik vertraut. Zusätzlich können Sie mit Ihrem erarbeiteten Wissen eine forensische Sicherung und Analyse des Hauptspeichers durchführen und sind sich den fallbezogenen Risiken bewusst. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit den forensischen Tools und können wichtige Ergebnisse daraus eigenständig entnehmen. Sie sind mit den Grundprinzipien der IT-Forensik vertraut und können diese bei einer forensischen Untersuchung anwenden. Des Weiteren können Aufgaben und spezfische Problemstellungen nachvollzogen und gelöst werden. *Sozialkompetenz:* Die Studierenden erlernen aufgrund gemeinsamer forensischen Untersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebunden Diskussion lösen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit eine forensische Untersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiter besitzen Sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.
Häufigkeit des Angebots:	Wintersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Eigenes Skript • Eoghan Casey (Hrsg.): Handbook of computer crime investigation. Forensic tools and technology. 6th Printing. Elsevier Academic Press, Amsterdam u. a. 2007, ISBN 978-0-12-163103-1. • Alexander Geschonneck: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. dpunkt Verlag, Heidelberg 2011, ISBN 978-3-89864-774-8. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Compilerbau

Modulbezeichnung:	Compilerbau
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Compilerbau
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Dr. Werner Massonne
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module, insbesondere: • Systemnahe Programmierung • Algorithmen und Datenstrukturen
Empfohlene Voraussetzungen:	• Theoretische Informatik
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 5
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalt und Niveau:	Im Modul Compilerbau wird auf folgende Themengebiete eingegangen: • Anwendungsgebiete und Aufbau von Compilern • Lexikalische Analyse auf Basis von regulären Sprachen • Syntaktische Analyse auf Basis von kontextfreien Grammatiken • Semantische Analyse durch attributierte Grammatiken und syntaxgesteuerte Definitionen, Erzeugung von Zwischencode • Optimierung und Codeerzeugung • Entwicklungswerkzeuge: Scannergenerator Flex und Parsergenerator Bison Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die Funktionsweise und Arbeitsschritte von Compilern. Sie können die theoretischen Konzepte erklären, die benötigt werden, um ausgehend von einer formalen Sprachdefinition einen Compiler zu konstruieren. Mit Hilfe der Tools Flex und Bison können die Studierenden selbst Compiler für realistische Einsatzszenarien erzeugen. *Methodenkompetenz:* Die Studierenden beherrschen die Methodik, für eine gegebene Quellsprache und eine gewünschte Zielsprache einen phasenbasierten Compiler zu bauen. Dabei kommen gewöhnlich Tools zur Anwendung, die eine starke Unterstützung bei der Umsetzung der theoretischen Modelle bieten. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die eigene Arbeitsweise und die Arbeitsweise anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Häufigkeit des Angebots:	Wintersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Übersetzerbau Band 2: Syntaktische und semantische Analyse, Reinhard Wilhelm, Helmut Seidl, Sebastian Hack, Springer Verlag, 2012 • Flex und Bison, John Levine, O'Reilly Media, 2009 • Compilerbau Teil 1+2, Alfred V. Aho, Ravi Sethi, Jeffrey D. Ullman, Oldenbourg Wissenschaftsverlag, 1999 • Übersetzerbau, Ralf Hartmut Güting and Martin Erwig, Springer Verlag, 1998 Weitere Literatur wird in der Lehrveranstaltung bekanntgegeben.

Netzsicherheit 1

Modulbezeichnung:	Netzsicherheit 1
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Netzsicherheit 1
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Lehrende:	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module insbesondere: • Programmierung 1a • Kryptologie 1
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Fachliteratur in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 3
Generelle Zielsetzung des Moduls:	

Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h
Lerninhalt und Niveau:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei wer-den sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asym-metrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen betrachtet, und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • Einführung in lokale Netze, • WLAN (IEEE 802.11), • VPN (IPSec, PPTP, IP Multicast), • Mobilfunk (GSM, UMTS), Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzu-stellen.

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erkennen die wichtigen Strukturen von Sicherheitsmechanismen in lokalen Datennetzen, verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln. Die Studenten können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	
Literatur:	• Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Computer Networks, Andrw S. Tanenbaum, 2002 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Kryptographie 2

Modulbezeichnung:	Kryptographie 2
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Kryptographie 2
Modulverantwortliche(r):	Prof. Dr. Christof Paar
Lehrende:	Prof. Dr. Christof Paar
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch, Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 5
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h

Lerninhalt und Niveau:	In diesem Modul werden asymmetrische kryptographische Verfahren behandelt. Die Schwerpunkte dieses Moduls liegen auf der Besprechung von praktisch wichtigen Verfahren und deren Einsatz für asymmetrische Basisdienste. Es werden sowohl diskrete Logarithmusverfahren (Diffie-Hellman, Elgamal, elliptische Kurven), als auch das RSA-Verfahren behandelt. Außerdem werden digitale Signaturen eingeführt. Es werden die Grundlagen der symmetrischen und asymmetrischen Schlüsselverteilung behandelt. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die Bedeutung von asymmetrischen kryptographischen Verfahren und verstehen die Strukturen der prominentesten asymmetrischen Primitiven. Darüber hinaus verstehen die Studenten die Sicherheitskonzepte und diverse Angriffsziele in der asymmetrischen Kryptographie. Die Studenten können ihr Wissen über die Kryptographie anwenden und Sicherheitslösungen finden. *Methodenkompetenz:* Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von asymmetrischen Verfahren nachvollziehen. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen von symmetrischen kryptographischen Verfahren aus und diskutieren Lösungswege von Problemen. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit aktuelle asymmetrische kryptographische Verfahren zu verstehen und eine fundierte Meinung über die Sicherheit dieser Verfahren zu vertreten. Darüber hinaus besitzen die Studierenden alle Voraussetzungen neue asymmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen einzuschätzen. Das umfangreiche Wissen der Studenten befähigt sie Sicherheitslösungen zu finden und einzusetzen.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Handbook of Applied Cryptography, Alfred J. Menezes, Paul C van Oorschot, Scott A Vanstone, 1996 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Realisierung von Softwareprojekten

Modulbezeichnung:	Realisierung von Softwareprojekten
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Realisierung von Softwareprojekten
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Hans-Georg Eßer
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module, insbesondere • Grundlagen der Programmierung • Programmierkonzepte • Konzeptionelle Modellierung
Empfohlene Voraussetzungen:	Keine
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 6
Generelle Zielsetzung des Moduls:	Zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalt und Niveau:	Im Modul Realisierung von Softwareprojekten wird auf folgende Themengebiete eingegangen: • Model Driven Architecture - UML • Sichere Softwareentwicklung SDL / Microsoft • JavaScript • Grundlegende Kenntnisse in PHP Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über Prozessmodellierung und lernen Zustandsdiagramme zu erstellen. Darüber hinaus erlangen sie Kenntnisse über Secure Coding Policies und Testing Policies. *Methodenkompetenz:* Die Studierenden beherrschen die Fähigkeiten ein Softwareprojekt zu entwerfen und umzusetzen sowie ein sicheres Programm zu schreiben. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Durch die Eigenentwicklung von Softwareprojekten erweitern die Studierenden ihre Selbstständigkeit. Die Studierenden lernen somit Verantwortung für ihr Handeln zu übernehmen und steigern ihre Entscheidungsfähigkeit.
Häufigkeit des Angebots:	Sommersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer
Literatur:	Als Begleitende und vertiefende Literatur wird empfohlen: • J. Ludewig, H. Lichter: Software Engineering, dpunkt.verlag 2013, ISBN: 978-3-86490-092-1 • I. Sommerville: Software Engineering, 9th ed., Pearson 2011, ISBN: 978-0-13-705346-9 Weitere Literatur wird in der Lehrveranstaltung bekanntgegeben

Netzsicherheit 2

Modulbezeichnung:	Netzsicherheit 2
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Netzsicherheit 2
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Lehrende:	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module insbesondere: • Modul Grundlagen der Programmierung • Modul Kryptographie 1 • Modul Kryptographie 2
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Fachliteratur in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 6
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h

Lerninhalt und Niveau:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen der dritten und vierten Ebene des OSI Schichtenmodells betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • SSL, • SSH, • OpenPGP, • S/MIME und • DNSSEC Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen. Als Grundlage werden kurz auch die Transportprotokolle TCP und UDP behandelt. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Teilnehmer erwerben die Grundlagen zum Einrichten sicherer Kommunikationskanäle. Darüber hinaus lernen sie verschiedene Wege, wie die einzelnen Anwendungen in der Vergangenheit angegriffen wurden. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.*Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein "gesundes Misstrauen"gegenüber vorgegebenen Sicherheitskonzepten.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum

Literatur:	• Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Computer Networks, Andrew S. Tanenbaum, 2002 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Netzsicherheit 3

Modulbezeichnung:	Netzsicherheit 3
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Netzsicherheit 3
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Lehrende:	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	• Modul Grundlagen der Programmierung
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Facharktikel in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 7
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h

Lerninhalt und Niveau:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung des World Wide Web (www) betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • Same Origin Policy • Cross Site Scripting • Cross Site Request Forgery • XML • Web Services Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben grundlegendes Wissen im Bereich der Sicherheit von Webanwendung. Sie sind in der Lage die Sicherheit einer Webanwendung einzuschätzen und Angriffspunkte offenzulegen. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein "gesundes Misstrauen"gegenüber vorgegebenen Sicherheitskonzepten.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum

Literatur:	• Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 • Computer Networks, Andrew S. Tanenbaum, 2002 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Weiterführende Themen der Computerforensik

Modulbezeichnung:	Weiterführende Themen der Computerforensik
Studiengang:	Bachelor Informatik / IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Lehrveranstaltungen und Lehrformen:	Weiterführende Themen der Computerforensik
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Einführung in die digitale Forensik
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 5
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 30 Zeitstunden Fernstudienanteil: 120 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: • Software Reverse Engineering. • Erkennen und Bewerten verschiedenster Informationsquellen • Informationsverknüpfung im Strafverfahren • Allgemeine Vorgehensweisen bei der Durchführung forensischer Analysen. • Bewertung digitaler Beweise auf Relevanz (technisch, juristisch). • Analyse von Festplattenabbilder und effizientes Auffinden gelöschter Informationen. • Möglichkeiten und Techniken der Antiforensik. • Praktische Bearbeitung von Aufgaben Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden haben Kenntnis über die Entstehung, der Manipulier- und Kopierbarkeit sowie der Personenbezogenheit von digitalen Spuren. Des weiteren haben Sie Kenntnis über Methoden der Antiforensik und können dies bei der Analyse berücksichtigen. Sie wissen um versteckte Bereiche, wie HPO und DCO auf einer Festplatte. Sie können unbekannte Datenformate analysieren und haben Kenntnis über das Vorgehen beim Software Reverse Engineering. Die Studierenden kennen weiter das grundlegende Konzept sowie die Eigenschaften der DOS und GPT Partitionen und der FAT und NTFS Dateisysteme und können mit diesem Wissen eine Dateisystemanalyse durchführen. Die Studierenden haben ein Verständnis, wie große Informationsmengen gemanagt und im Strafverfahren verknüpft werden. *Methodenkompetenz:* Die Studierenden können Fragen zu den oben genannten Fachkompetenzen schriftlich beantworten. Sie können Festplatten mit den Dateisystemen FAT und NTFS analysieren. Sie können unbekannte Software anhand von Software Reverse Engineering analysieren. Sie können digitale Beweise verschiedenster Informationsquellen bewerten und können angewandte Methoden der Antiforensik bei der Analyse erkennen. Sie können im Strafverfahren große Informationsmengen miteinander verknüpfen und Wissen um die Handhabe großer Informationsmengen. *Sozialkompetenz:* Die Studierenden sind in der Lage als Team zusammenzuarbeiten und so Lösungen für die gestellten Aufgaben zu finden. Darüber hinaus können Sie zu den Themen eine fachgebundene Diskussion führen. *Selbstkompetenz:* Die Studierenden sind in der Lage die Lösungen zu den Aufgaben und Problemen mündlich und schriftlich zu formulieren und zu präsentieren. Dadurch könne Sie sich auch gegen Einwände in einer Diskussion verteidigen. Sie sind in der Lage selbständig geeignete Literatur zu finden und einzusetzen.
Häufigkeit des Angebots:	Sommersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Eigenes Skript • Eoghan Casey (Hrsg.): Handbook of computer crime investigation. Forensic tools and technology. 6th Printing. Elsevier Academic Press, Amsterdam u. a. 2007, ISBN 978-0-12-163103-1. • Alexander Geschonneck: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. dpunkt Verlag, Heidelberg 2011, ISBN 978-3-89864-774-8. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Kryptographische Protokolle

Modulbezeichnung:	Kryptographische Protokolle
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann als Wahlpflichtmodul gewählt werden, und ist kein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Kryptographische Protokolle
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Lehrende:	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	• Modul Kryptographie 1 • Modul Kryptographie 2
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Facharktikel in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 6
Generelle Zielsetzung des Moduls:	Modul zum Aufbau von Kenntnissen und Erfahrungen in einem Spezialgebiet
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h

Lerninhalt und Niveau:	Dieses Modul bietet eine Einführung in das Gebiet der kryptographischen Protokolle, die den Einsatz bekannter und neuer Verfahren der Kryptographie in der Kommunikation zwischen mehreren Instanzen beschreiben. Hierbei wird sowohl Wert auf die Beschreibungen als auch auf die Sicherheit gelegt. Das Modul umfasst als Einführung allgemeine kryptographische Grundlagen, die Konzepte der beweisbaren Sicherheit und eine Einführung zu kryptographischen Protokollen. Im Folgenden werden einfache Protokolle behandelt. Hierzu zählen Passwort/Nutzername Protokolle, Wechselcodes, das Challenge-and-Response Verfahren, das Diffie-Hellman Protokoll, ElGamal sowie Shamir's No-Key-Verfahren. Des Weiteren werden Zero Knowledge Protokolle und ihre Theorie besprochen. Den Schwerpunkt des Moduls werden Schlüsselaustausch Protokolle bilden. Hierfür werden die Sicherheitsmodelle von Belare - Rogaway sowie Canetti - Krawczyk eingeführt. Den Abschluss des Moduls bildet eine detaillierte Beschreibung und formale Sicherheitsanalyse von TLS, dem wohl am weitesten verbreitete Authentifizierungs- und Schlüsseltausch Protokolls im Internet. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden verstehen die Besonderheit kryptographischer Protokolle, bei denen nicht mehr ein Algorithmus im Vordergrund steht, sondern die Interaktion verschiedener Einheiten. Die Studenten erkennen die praktische Relevanz der Kryptographie und begreifen die Schwierigkeit, kryptographische Protokolle - wie sie im Internet eingesetzt werden - formal auf ihre Sicherheit hin zu analysieren. Die Studenten kennen wichtige Sicherheitsziele und Sicherheitsmodelle, welche sie auf echte Protokolle anwenden können. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit kryptographischer Fachliteratur und können ihr wichtige Ergebnisse eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Beweistechniken und Sicherheitsmodellen vertraut, welche für formale Sicherheitsanalysen neuer Protokolle angewendet werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen und Anwenden von neuen Modellen und Techniken aus und können wissenschaftlich zielorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, kryptographische Protokolle zu analysieren und eine wissenschaftlich begründete Einschätzung ihrer Sicherheit zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Protokolle aus der aktuellen Fachliteratur zu verstehen und ihre Sicherheit eigenständig zu evaluieren.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	

Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Online-material in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• Moderne Verfahren der Kryptographie, Beutelsbacher, Schwenk, Wolfenstetter, 2000 • Protocols for Authentication and Key Esteblishment, Boyd, Maturia, 2003 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Sicherheit mobiler Systeme

Modulbezeichnung:	Sicherheit mobiler Systeme
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul ist ein Wahlpflichtmodul.
Lehrveranstaltungen und Lehrformen:	Sicherheit mobiler Systeme
Modulverantwortliche(r):	Prof. Dr. Thorsten Holz
Lehrende:	Prof. Dr. Thorsten Holz
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	• Programmierung • Kryptographie • Netzsicherheit 1-3
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Fachartikel teilweise in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 6
Generelle Zielsetzung des Moduls:	

Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h
Lerninhalt und Niveau:	In diesem Modul erwerben die Teilnehmer Kenntnisse über Sicherheitsaspekte von verschiedenen mobilen Systemen, insbesondere zur Sicherheit von Smartphones. Im ersten Teil des Moduls liegt der Schwerpunkt auf der Beschreibung der wichtigsten Sicherheitsfunktionen von mobilen Systemen. Im zweiten Teil des Moduls wird die Sicherheit von Smartphones genauer beleuchtet und verschiedene Sicherheitsaspekte werden genauer betrachtet, der Fokus liegt dabei auf Apps für Smartphones. In der Vorlesung werden verschiedene Sicherheitsaspekte von mobilen Systemen vorgestellt. Anhand von konkreten Beispielen wird erläutert, wie verschiedene Arten von mobilen Systemen aufgebaut sind und welche Sicherheitsrisiken diese besitzen. Dies umfasst unter anderem die folgenden Themen: • Design von GSM und UMTS (Sicherheitsaspekte, Lokalisierungsverfahren, Verbindungsmanagement) • Sicherheit von Satellitentelefonen (GMR) • Sicherheitsaspekte von DECT • Design mobiler Betriebssysteme (Android und iOS) • Analyse von (mobilen) Apps

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erlernen die wichtigen Strukturen von Sicherheitsaspekten in mobilen Datennetzen, verstehen die darin verwendeten kryptographischen Verfahren sowie das Zusammenspiel verschiedener Protokolle. Die Studierenden können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern. Dazu werden auch konkrete Angriffe auf existierende Systeme vorgestellt, um ein tiefergehendes Verständnis zu erlangen. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit (englischer) Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffs- und Analysetechniken vertraut, welche auf neue Systeme, Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studierenden tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. Die konstruktive Diskussion wird im Rahmen von Übungen erlernt. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit, sich selbständig eine Meinung über die Sicherheit von verschiedenen mobilen Systemen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studierenden entwickeln ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	
Literatur:	• Hannes Federrath: Sicherheit mobiler Kommunikation: Schutz in GSM-Netzen, Mobilitätsmanagement und mehrseitige Sicherheit, Vieweg, 1999 • Noureddine Boudriga: Security of Mobile Communications, Auerbach Publications, 2009 • Miller et al.: iOS Hacker's Handbook, Wiley, 2012 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Sicherheitsmanagement

Modulbezeichnung:	Sicherheitsmanagement
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Lehrveranstaltungen und Lehrformen:	Sicherheitsmanagement
Modulverantwortliche(r):	Dr. Christoph Wegener
Lehrende:	Dr. Christoph Wegener
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Seminar-/Hausarbeit
Berechnung der Modulnote:	Schriftliche Prüfung in Form einer Seminar-/Hausarbeit
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	Grundlegende Kenntnisse in den allgemeinen Aspekten der Informationssicherheit.
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Fachartikel in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 7
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 15 h • Vorlesungsteil: 12h • Übungsteil: 3 h Eigenstudium: 135 h • Durcharbeiten der Studienbriefe: 50 h • Durcharbeiten der Sekundärliteratur: 35 h • Ausarbeiten der Seminar-/Hausarbeit: 50 h

Lerninhalt und Niveau:	Das Kapitel *Einführung und Motivation* soll den Studierenden zunächst die notwendigen Grundlagen vermitteln und für die Grundideen und –ziele der Informationssicherheit motivieren. Dabei werden die Hauptziele der Informationssicherheit dargestellt, vor allem auch im Vergleich zu denen der IT-Sicherheit. Im Kapitel *Governance in der Informationssicherheit* lernen die Studierenden anschließend die wesentlichen Konzepte und Ideen der Governance im Bereich der Informationssicherheit kennen. Dabei werden sowohl die grundlegenden Elemente der Governance behandelt, zudem wird aufgezeigt, wie eine effektive Governance betrieben werden kann. Im Kapitel *Grundlagen des Risikomanagements* erlernen die Studierenden die Grundzüge des Risikomanagements kennen. Nach einem einleitenden Teil, der unter anderem die grundlegenden Begrifflichkeiten vermitteln, wird aufgezeigt, wie der Prozess des Risikomanagements im Bereich der Informationssicherheit betrieben werden sollte. Nach diesen einführenden Überlegungen gliedert sich das Kapitel *Entwicklung und Management eines Programms zur Informationssicherheit* in zwei Abschnitte. • Zunächst wird der Prozess der *Entwicklung* eines Programms zur Informationssicherheit behandelt. Hier erlernen die Studierenden, aus welchen Komponenten ein Programm zur Informationssicherheit besteht und was beim Aufbau eines solchen beachtet werden muss. • Anschließend wird auf das Thema *Management* eines Programms zur Informationssicherheit eingegangen. Dabei erlernen die Studierenden, wie ein Programm zur Informationssicherheit aufrecht erhalten werden kann und welche Prozesse dafür aufzubauen sind. Insbesondere wird auch thematisiert, wie die zur Verfügung stehenden Ressourcen möglichst effizient eingesetzt werden können. Im Abschnitt *Grundlagen des Incident Management* erlernen die Studierenden, was im "Falle des Falles" zu tun ist. Dabei werden vor allem die Vorkommnisse behandelt, die im Rahmen des Risikomanagements nicht bzw. nicht ausreichend berücksichtigt werden konnten und die somit "unvorhergesehene" Ereignisse darstellen. Abschließend erlernen die Studierenden im Kapitel *Informationssicherheitsmanagement auf Basis von BSI IT-Grundschutz* den Aufbau eines Informationssicherheits-Managementsystems auf Basis von BSI IT-Grundschutz kennen. Dabei wird die Vorgehensweise anhand von konkreten Fallbeispielen exemplarisch erarbeitet. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die grundlegenden Aspekte der Informationssicherheit und des Managements der Informationssicherheit, insbesondere in den Bereichen Governance in der Informationssicherheit, Risikomanagement, Incident Response Management und den Grundlagen des BSI IT-Grundschutzes. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Problematiken im Rahmen des Managements von Informationssicherheit vertraut und können dieses Wissen an Praxisbeispielen umsetzen. *Sozialkompetenz:* Durch Erarbeitung von Fragestellungen in der Gruppe lernen die Studierenden die Sichtweisen verschiedener Bereiche der Informationssicherheit kennen und einen entsprechenden Ausgleich der Interessen zwischen den beteiligten Parteien im Unternehmen herbeizuführen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit, Informationssicherheit zu managen und sich in diesem Bereich selbständig weiter zu bilden bzw. zu entwickeln. Darüber hinaus erlangen sie die Kompetenz, dieses Wissen an die sich ständig ändernden Bedingungen im Unternehmen anzupassen.
Häufigkeit des Angebots:	Jährlich
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Online-Materialen in der Lernplattform, ggf. unterstützende Übungen über die Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• BSI Standards zum IT-Grundschutz (insbesondere der Standard BSI 100-1) • Grundlagen der ISO 27000 Serie • Praxisbuch zur ISO/IEC 27001 • Diverse Leitfäden der ISACA Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Spam

Modulbezeichnung:	Spam
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul ist ein Wahlpflichtmodul.
Lehrveranstaltungen und Lehrformen:	Spam
Modulverantwortliche(r):	Dr. Christopher Wolf
Lehrende:	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Facharktikel in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 7
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h

Lerninhalt und Niveau:	E-Mails bilden heutzutage einen wichtigen Kommunikationskanal. Vor diesem Hintergrund stellt das immer stärker werdende Aufkommen von Spam nicht nur ein ärgernis dar, sondern verursacht auch einen enormen wirtschaftlichen Schaden. Um zu verstehen, wie Spam entsteht, werden zum einen Grundlagen vermittelt, wie die Wort-Ethymologie, die verschiedenen Formen von Spam in unterschiedlichen Medien, die oft verwendeten Definitionen sowie die in der Vorlesung verwendete Definition. Zum anderen werden in einer Fall-Studie das Wirtschaftsmodell sowie die Enttarnungsmöglichkeiten von Spammern besprochen. Ein tieferer Einblick in das SMTP-Protokoll stellt den Protokollfluss zwischen Sender und Empfänger dar und beschreibt die Verlässlichkeit der verschiedenen im E-Mail-Quellcode enthaltenen Daten und deren Manipulationsmöglichkeiten in Form einer Analyse der Header-Felder. Es werden verschiedene Formen der Anti-Spam-Maßnahmen präsentiert. Darunter fallen einfache Methoden wie Black- und Whitelists sowie die daraus resultierenden und leicht abgewandelten Graylists. Ebenfalls werden fortgeschrittene Methoden von Grund auf besprochen, wie bspw. Bayessche Filter. Als weitere Anti-Spam-Techniken werden auch alternative Protokolle angesprochen, die Zeit- und Speicherbeweise als Funktionen einsetzen, ebenso wie SPK und DKIM. Weiterhin wird Spam vom juristischen Standpunkt aus betrachtet, wobei das Opt-In bzw. Opt-Out-Verfahren im Fokus liegt. Ebenso werden die Strafbarkeit sowie die zivilrechtlichen Ansprüche und deren Durchsetzbarkeit angesprochen. Hier wird auch das Spam-Verständnis in den USA mit dem der EU verglichen. Weiterhin werden die juristischen Möglichkeiten für Whitelists diskutiert. Im wirtschaftlichen Bereich werden die Preise für E-Mail, die Wirtschaftlichkeit von Spam sowie der Verfolgungsdruck von Spammern behandelt. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben grundlegendes Wissen im Bereich der Email-Kommunikation. Sie sind in der Lage Spam- und Anti-Spam Techniken zu erläutern und kennen rechtliche Aspekte von Spam. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Sie verstehen die Wirksamkeit von Spam-Filtern und können diese konfigurieren. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit Techniken im Spam-Umfeld aktueller Fachliteratur zu entnehmen und ihre Bedeutungen zu evaluieren.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	

Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

Netzbasierte Angriffserkennung

Modulbezeichnung:	Netzbasierte Angriffserkennung
Studiengang:	Bachelor Informatik / IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Lehrveranstaltungen und Lehrformen:	Netzbasierte Angriffserkennung
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Netzsicherheit 1
Empfohlene Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Netzsicherheit 2
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Technische Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 5
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 30 Zeitstunden Fernstudienanteil: 120 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalt und Niveau:	In diesem Modul werden die folgenden Themengebiete behandelt: • Typische netzbasierte Angriffe. • Datenquellen und -formate für netzbasierte Angriffserkennung (OpenFlow, NetFlow, IPFIX) • Schadsoftware. • Maschinelle Lernverfahren zur Angriffserkennung. • Reaktionsmöglichkeiten. • Moderne Netzwerkparadigmen wie Software-Defined Networking (SDN). • Praktische Bearbeitung von Aufgaben. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die Grundlagen der Netzsicherheit sowie typische netzbasierte Angriffe. Sie haben Kenntnis über die Platzierung von Sensoren im Netzwerk sowie über Datenformate für netzbasierte Angriffserkennung. Sie können die Vor- und Nachteile von Deep Packet Inspection gegenüber aggregierten Formaten wie NetFlow bzw. IPFIX bewerten. Die Studierenden verstehen, wie unterschiedliche Malware-Samples netzbasierte Angriffe durchführen. Sie kennen die Funktionsweise von Maschinellen Lernverfahren und können deren Einsatz für die Klassifikationsprobleme bewerten. Die Studierenden kennen Detektionsverfahren zur netzbasierten Angriffserkennung und wissen, wie man auf unterschiedliche Angriffe reagiert. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit gängigen Tools für maschinelles Lernen und können wichtige Ergebnisse daraus eigenständig bewerten. Sie sind mit den Grundprinzipien der netzbasierten Angriffserkennung mittels NetFlow oder IPFIX vertraut und können diese bei einer Angriffserkennung anwenden. Sie können weiter mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen aufgrund gemeinsamer Angriffsuntersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebunden Diskussion lösen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit eine Angriffsuntersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiter besitzen Sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.
Häufigkeit des Angebots:	Wintersemester
Anerkannte Module:	

Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Eigenes Skript • C. Bishop: Pattern Recognition and Machine Learning. Information Science and Statistics. Springer, Berlin 2008, ISBN 978-0-3873-1073-2. • L. Bilge, D. Balzarotti, W. Robertson, E. Kirda, C. Kruegel: Disclosure: detecting botnet command and control servers through large-scale NetFlow analysis. Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC 2012), p. 129-138, ACM New York, NY, 2012. ISBN: 978-1-4503-1312-4 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

User-Centered Security

Modulbezeichnung:	User-Centered Security
Studiengang:	Bachelor Informatik / IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Lehrveranstaltungen und Lehrformen:	User-Centered Security
Modulverantwortliche(r):	Prof. Dr. Marian Margraf
Lehrende:	Prof. Dr. Marian Margraf
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	keine
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Fachliteratur in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 6
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 1 h • Prüfung: 1 h Eigenstudium: 149 h • Durcharbeiten der Studienbriefe: 100h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 30h • Individuelle Prüfungsvorbereitungen: 10h

Lerninhalt und Niveau:	User-Centered Security befasst sich mit der Benutzerfreundlichkeit und Sicherheit von Systemen. In diesem Modul werden die grundlegenden Problemen betrachtet, die auftreten, wenn ein System zugleich benutzerfreundlich und sicher sein soll. Es wird diskutiert, warum benutzerzentrierte Sicherheit überhaupt ein erstrebenswertes Ziel ist und wie sie in Softwareentwicklungsprozesse eingebunden werden kann. Dabei werden die wissenschaftlichen Methoden zur Untersuchung von Systemen und dem Umgang damit erlernt und es werden exemplarisch die Bereiche Authentifizierung und Internetsicherheit besprochen. Im Zusammenhang mit der benutzerzentrierten Authentifizierung werden die Schwächen von Passwörtern und mögliche Alternativen, wie grafische Passwörter, biometrische Verfahren und Mehrfaktorauthentifizierung untersucht. Im Bereich der Internetsicherheit werden Schwierigkeiten bei der Verwendung von PKIs, OpenPGP und dem Design von Warnmeldungen untersucht und daran allgemeine Verbesserungsmöglichkeiten vermittelt. Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden verstehen die der User-Centered Security zugrunde liegenden Probleme. Sie können Systeme im Hinblick darauf untersuchen und beurteilen, wie weit Kriterien der User-Centered Security bedacht und umgesetzt worden sind. Sie können zudem geeignete Entwicklungsprozesse für eigene Systeme einsetzen, die die Aspekte der User-Centered Security beachten. Die Studierenden sind dafür mit den grundlegenden Wissenschaftlichen Methoden dieses Bereichs vertraut. *Methodenkompetenz:* Die Studierenden können mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen die fachgebundene Diskussion, die sich aus der gemeinsamen Teamarbeit zum Lösen von Aufgaben ergeben. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Themen von User-Centered Security zu bilden und besitzen darüber hinaus die Kompetenz sie in den entsprechenden Gebieten der Informatik einsetzen zu können.
Häufigkeit des Angebots:	Sommersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Zurko, M.; Simon, R.: User-Centered Security, 1996 • Cranor, L.; Garfinkel, S.: Security and Usability: Designing Secure Systems That People Can Use, ISBN 978-0-596-00827-7, O'Reilly, 2005 • Garfinkel, S.; Lipfort, H.: Usable Security: History, Themes, and Challenges, ISBN SBN: 978-1-627-05529-1, Morgan & Claypool, 2014 • Lazar, J.; Feng, J.; Hochheiser, H.: Research Methods in Human-Computer Interaction, ISBN 978-0-470-72337-1, Wiley, 2010 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Incident Management

Modulbezeichnung:	Incident Management
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann als Wahlpflichtmodul gewählt werden.
Lehrveranstaltungen und Lehrformen:	Incident Management
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 4
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalt und Niveau:	Im Modul Incident Management wird auf folgende Themengebiete eingegangen: • Grundwissen des Incident Management • IT-Service Management (ITSM) • IT-Security Management • Risikomanagement Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erlangen mit diesem Modul das Basiswissen über das Incident Management und das Risikomanagement. Sie können die Schritte des Incident Management Prozesses nachvollziehen und sind imstande grundlegende Begriffe des Incident Management zu erklären und einzuordnen und können zwischen den spezifischen Rollen im Incident Management differenzieren. Ferner sind die Studierenden in der Lage einen Risikomanagementprozess mit seinen einzelnen Phasen zu erklären und kennen die bekannten Methoden und Werkzeuge des Risikomanagements. *Methodenkompetenz:* Die Studierenden sind in der Lage den Incident Management Prozess selber anzuwenden und eine Risikoberechnung aus der Wahrscheinlichkeit und der Schadenshöhe durchzuführen. Ferner können die Studierenden die einzelnen Schritte des Risikomanagementprozesses nachvollziehen und anwenden. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden haben sich ein Grundwissen über das Incident Management angeeignet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Häufigkeit des Angebots:	in jedem Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	• IT-Sicherheit: Konzepte - Verfahren - Protokolle, Claudia Eckert, 2006 • Moderne Betriebssysteme, Andrew S. Tanenbaum, 2003 • Betriebssysteme - Prinzipien und Umsetzung, William Stallings, 2005 • Malware, Eugene Kaspersky, 2008 • Computer Security, Dieter Gollmann, 2010 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Elektronische Identitäten

Modulbezeichnung:	Elektronische Identitäten
Studiengang:	Bachelor Informatik / IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Lehrveranstaltungen und Lehrformen:	Elektronische Identitäten
Modulverantwortliche(r):	Prof. Dr. Marian Margraf
Lehrende:	Prof. Dr. Marian Margraf
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	keine
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Fachliteratur in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 6
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 1 h • Prüfung: 1 h Eigenstudium: 149 h • Durcharbeiten der Studienbriefe: 100h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 30h • Individuelle Prüfungsvorbereitungen: 10h

Lerninhalt und Niveau:	Auf folgende Themengebiete wird eingegangen: • Grundprinzipien von elektronischen Identitäten • Kryptographische Grundlagen für elektronische Identitäten • Hoheitliche elektronische Identitäten (z. B. elektronische Ausweise, Reisepässe) • Elektronische Identitäten in Netzwerken (z. B. PKIs, OpenID, OAuth) • Elektronische Identitäten in Organisationen (z. B. SSO-Systeme, Identitätsmanagement) Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben ein Verständnis für die grundlegenden Konzepte von elektronischen Identitäten. Sie kennen weit verbreite Verfahren und können neue Verfahren untersuchen und beurteilen. *Methodenkompetenz:* Die Studierenden können mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen die fachgebundene Diskussion, die sich aus der gemeinsamen Teamarbeit zum Lösen von Aufgaben ergeben. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Thematik der elektronischen Identitäten zu bilden und besitzen darüber hinaus die Kompetenz sie in den entsprechenden Gebieten der Informatik einsetzen zu können.
Häufigkeit des Angebots:	Wintersemester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	
Literatur:	Die empfohlene Literatur wird in der Lehrveranstaltung bekannt gegeben.

Ethisches Hacking

Modulbezeichnung:	Ethisches Hacking
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann als Wahlpflichtmodul gewählt werden.
Lehrveranstaltungen und Lehrformen:	Ethisches Hacking
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	Module Rechnerstrukturen und Systemsicherheit, Netzwerk-Kenntnisse (Technik und grundlegende Protokolle)
Empfohlene Voraussetzungen:	Module Rechnerstrukturen und Systemsicherheit, Netzwerk-Kenntnisse (Technik und grundlegende Protokolle)
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 4
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalt und Niveau:	Im Modul Ethical Hacking wird auf folgende Themengebiete eingegangen: • Definition und Anwendung der Begriffe Angriff, Hacking, Hacker, Ethisches Hacking und Cyberkriminalität • Taktische Prinzipien und das Dilemma des Verteidigers • Tätermotivation und Zielauswahl • Die Anatomie des möglichen Opfers • Reconnaissance und automatisierte Informationsbeschaffung • DNS-Enumeration, DNS-Cache Snooping • Fingerprinting und Schwachstellenermittlung • Google als Hacking Tool • Social Engineering • Schwachstellenermittlung an einem Zielsystem • Ausführung eines Angriffs und Kompromittierung des Systems • Spurenbeseitigung • Technische und nicht-technische Methoden des ethischen Hackings • Techniken, Tools und Anwendungsbeispiele Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die fundamentalen Begriffe und Prinzipien, welche die Gefahrensituation eines Computersystems beschreiben. Sie sind in der Lage Interessengruppen für die Angriffe auf IT-Infrastrukturen zu identifizieren und deren zentrale Handlungsprinzipien sowie Strategien darzustellen. Darüber hinaus können sie die grundlegenden Positionen und ethische Handlungslinien der Verteidiger charakterisieren, welche deren Basis der digitalen Selbstverteidigung bilden. Die Studierenden sind in der Lage, die Phasen eines Hacking-Angriffs zu skizzieren und deren strukturelle Chronologie zu beschreiben. Sie können die Vorgehensweise der Hacker in jeder einzelnen Phase in ihrer Methode und den verwendeten Technologien, Protokollen und Tools beschreiben. Darüber hinaus sind die Studierenden befähigt, verschiedene Angriffsformen zu charakterisieren und zu unterscheiden, sowie passende Verteidigungsstrategien zu benennen und geeignete Mittel und Wege aufzuzeigen. Sie verstehen die Wege der Informationsbeschaffung aus öffentlichen Quellen oder des Social Engineerings und den dabei verfolgten Angreiferprinzipien der Tarnung und Täuschung. *Methodenkompetenz:* Die Studierenden sind in der Lage den Gefährdungsgrad einer IT-Infrastruktur einzuschätzen und daraus ableitend die Voraussetzung für einen erfolgreichen Hacking-Angriff zu benennen und zu charakterisieren. Aus der bei Hacking-Angriffen verfolgten Chronologie und Methodik sind die Studierenden außerdem in der Lage Mittel und Strategien zur Früherkennung der jeweiligen Bedrohungsszenarien geeignete Schutzmaßnahmen zu skizzieren und anzuwenden. Dafür sind sie in der Lage, die dazu nötigen Tools auszuwählen und in einem Anwendungsszenario zielführend einzusetzen. Aus der Kenntnis der Durchführung eines erfolgreichen Angriffs auf ein computergesteuertes Informationssystem sind die Studierenden in der Lage einen solchen Angriff zu planen und im Zuge eines Sicherheitstests selbst auszuführen und dabei gleichzeitig ethische und rechtliche Leitlinien zu befolgen. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen. *Selbstkompetenz:* Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.
Häufigkeit des Angebots:	in jedem Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	• Michael T. Simpson, Kent Backman und James E. Corley. Ethical Hacking and Network Defense, Course Technology, 2013 • Sandro Gaycken. Cyberwar: Das Internet als Kriegsschauplatz. Open Source Press; 1. Auflage, 2010 • Johnny Long. Google Hacking for Penetration Testers, Syngress, 2008 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Anonymität im Netz

Modulbezeichnung:	Anonymität im Netz
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann als Wahlpflichtmodul gewählt werden.
Lehrveranstaltungen und Lehrformen:	Anonymität im Netz
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	Netzwerk-Kenntnisse (Technik und grundlegende Protokolle), Grundkenntnisse Kryptographie
Empfohlene Voraussetzungen:	Netzwerk-Kenntnisse (Technik und grundlegende Protokolle), Grundkenntnisse Kryptographie
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik
Einordnung ins Fachsemester:	Ab Studiensemester 4
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalt und Niveau:	Im Modul Anonymität im Netz wird auf folgende Themengebiete eingegangen: • Kommunikation in Netzwerken bei Anwesenheit innerer und äußerer Angreifer • Definition und Anwendung der Begriffe Anonymität, Unverkettbarkeit, Unbeobachtbarkeit • Konzepte von Unterscheidbarkeit, Verkettbarkeit und Pseudonymität • Privacy mit unterschiedlichem Schutzniveau von Kommunikationsdaten • Rechtliche Rahmenbedingungen von Anonymität und Datenschutz im Internet • Anonymisierungstechnologien, Overlay-Netzwerke • Anonymisierer, Digitales Mixen, Java Anon Proxy (JAP)/JonDo • TOR-Netzwerke und Hidden Services • Bedrohungsmodelle, Mechanismen zum Schutz privater Netzwerk-Kommunikation • Selbstschutz in sozialen Netzwerken, Deep Web und Kriminalität • Remailer-Systeme und OTR-Technologien • Techniken zur Identifizierung von Nutzern im Web • Auswirkungen der anonymisierten Internetnutzung Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die grundlegenden Begriffe und Konzepte der Anonymität und des Schutzes der Privatsphäre in Computer-Netzwerken. Sie können darüber hinaus Anonymität von schwächeren Formen der Sicherung vertraulicher bzw. identitätsbezogener Informationen unterscheiden. Die Studierenden sind in der Lage, unterschiedliche Angriffe auf anonyme Netzwerk-Kommunikation und den Austausch vertraulicher Daten zu beschreiben und Abwehrmechanismen zu erläutern. Sie haben Grundkenntnisse über Anonymisierungstechnologien wie Anonymisierer, Digitale Mixer, Remailer-Systeme und TOR-Netzwerke und können deren Funktionsweise erläutern sowie OTR-Technologien beschreiben. Zudem können die Studierenden mittels ihrer Kenntnisse über die Sicherheitsaspekte vernetzter Umgebungen, Mechanismen des digitalen Mixens und die Funktionsweise von Overlay-Netzwerken zu den jeweiligen Bedrohungsszenarien passende Schutzmaßnahmen und Tools zielführend einsetzen. *Methodenkompetenz:* Die Studierenden können Voraussetzungen und Umstände erläutern, die zum Erreichen von Anonymität in einem Netzwerk kommunizierender Teilnehmer erforderlich sind. Sie sind außerdem in der Lage ausgehend von unterschiedlichen Zielen einer Kommunikation über Computer-Netzwerke und verschiedenen Ebenen des Schutzbedarfs der übertragenen Informationen, nötige Protokolle und die passende Technologie auszuwählen, die zum Erreichen dieser Zwecke notwendig ist. Sie sind in der Lage Bedrohungsszenarien zu erkennen und zu analysieren, sowie notwendige Schutzmaßnahmen zu skizzieren und anzuwenden. Die Studierenden sind imstande das Für und Wider von Anonymität bei unterschiedlichen Standpunkten und Rechtsauffassungen von Freiheit und Verbrechensbekämpfung zu diskutieren und Lösungsansätze zu erörtern. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen. *Selbstkompetenz:* Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.
Häufigkeit des Angebots:	in jedem Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	• Helmut Bäumler, Albert von Mutius (Hrsg.): Anonymität im Internet: Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Vieweg 2003 • Phillip Brunst: Anonymität im Internet - rechtliche und tatsächliche Rahmenbedingungen, Duncker & Humblot, Berlin 2009 • Eric Siegel. Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die, John Wiley & Sons, 2013 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Internetforensik

Modulbezeichnung:	Internetforensik
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann als Wahlpflichtmodul gewählt werden.
Lehrveranstaltungen und Lehrformen:	Internetforensik
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	Einführung in die IT-Sicherheit, Rechnerstrukturen, Systemsicherheit
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik
Einordnung ins Fachsemester:	Ab Studiensemester 4
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalt und Niveau:	Im Modul Internetforensik wird auf folgende Themengebiete eingegangen: • Angriffsmöglichkeiten auf IT-Systeme • Interna von Websites, Webservern, Webbrowsern und Email • Möglichkeiten der digitalen Spurensuche • Techniken der Informationssuche Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden haben IT-forensische Grundlagen erworben, dazu gehören z.B. die wissenschaftliche Methodik, essentielle Prinzipien, Analyseansätze und Modelle zur Vorgehensweise bei der Spurensuche. Desweiteren haben sie einen Überblick über die unterschiedlichen Bedrohungen im Internet und die verschiedenen Angriffsmöglichkeiten bekommen. *Methodenkompetenz:* Die Studierenden können zwischen unterschiedlichen IT-Angriffsmöglichkeiten und Betrugsversuchen differenzieren und diese erklären. Desweiteren erlernen sie eine Vielzahl von Techniken zum Aufspüren der Websites und Server, die hinter Phishing, Spam und anderen Formen von Internet-Betrug sich verstecken und sind in der Lage diese anzuwenden. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden haben sich ein Grundwissen über IT-Forensik angeeignet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Häufigkeit des Angebots:	in jedem Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	• Internet Forensics, Robert Jones, 2005 • Real Digital Forensics, K. Jones, R. Bejtlich, C. Rose, 2005 • Computer Forensik, A. Geschonneck, 4. Auflage, 2010 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Seminar

Modulbezeichnung:	Seminar
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	berufsbegleitender Bachelorstudiengang IT-Sicherheit
Lehrveranstaltungen und Lehrformen:	Seminar
Modulverantwortliche(r):	Betreuender Dozent kann jeder Professor oder Lehrbeauftragter des Studiengangs sein.
Lehrende:	Betreuender Dozent kann jeder Professor oder Lehrbeauftragter des Studiengangs sein.
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Ausarbeitung im Umfang von 10-20 Seiten, mündliche Präsentation im Umfang von 45 Minuten
Berechnung der Modulnote:	
Notwendige Voraussetzungen:	• Proseminar • Studienleistungen im Umfang von mindestens 20 ECTS
Empfohlene Voraussetzungen:	Keine
Unterrichts- und Prüfungssprache:	Deutsch oder Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik
Einordnung ins Fachsemester:	Studiensemester 6, 7 oder 8
Generelle Zielsetzung des Moduls:	
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 1 h • Seminarvortrag: Präsentation und Diskussion Eigenstudium: 149 h • Themenbearbeitung • Besprechungen mit dem Betreuer • Vorbereitung der Präsentation

Lerninhalt und Niveau:	Der Themenbereich des Seminars wird vor dem Semester bekanntgeben. Jeder Studierende erhält ein individuelles Thema, in der Regel in Form eines initialen Papers. Von diesem ausgehend werden tiefere Literaturrecherchen zur Ergründung des Gesamtthemas durchgeführt. Die Ergebnisse werden nach den Kriterien wissenschaftlichen Arbeitens schriftlich ausgearbeitet und mündlich vor den Mitstudenten und Betreuern präsentiert. Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erweitern ihre im Proseminar erworbenen Kompetenzen. Sie können eine komplexere Fragestellung auf dem Gebiet der Informatik selbstständig recherchieren und ihre Ergebnisse präsentieren und verteidigen. *Methodenkompetenz:* Die Studierenden haben einen vertieften Einblick in die Methodiken wissenschaftlichen Arbeitens können diese Methodiken bei einem größeren, vorgegebenen Thema anwenden. *Sozialkompetenz:* Durch die Enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können komplexe fachbezogene Inhalte klar und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	
Literatur:	

Projekt

Modulbezeichnung:	Projekt
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	berufsbegleitender Bachelorstudiengang IT-Sicherheit
Lehrveranstaltungen und Lehrformen:	Projekt
Modulverantwortliche(r):	Betreuender Dozent kann jeder Professor oder Lehrbeauftragter des Studiengangs sein.
Lehrende:	Betreuender Dozent kann jeder Professor oder Lehrbeauftragter des Studiengangs sein.
Dauer:	2 Semester
Credits:	10 ECTS
Studien- und Prüfungsleistungen:	Kurze Schriftliche Ausarbeitung im Umfang von ca. 10 Seiten, mündliche Präsentation im Umfang von 30 Minuten und anschliessende Fachdiskussion im Umfang von 15 Minuten (Kolloquium)
Berechnung der Modulnote:	
Notwendige Voraussetzungen:	• Studienleistungen im Umfang von mindestens 20 ECTS. • Proseminar
Empfohlene Voraussetzungen:	Keine
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik
Einordnung ins Fachsemester:	Studiensemester 6 bis 8
Generelle Zielsetzung des Moduls:	
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 300 h Präsenzzeit: 1 h • Kolloquium Eigenstudium: 299 h • Themenbearbeitung • Besprechungen mit dem Betreuer • Vorbereitung der Präsentation

Lerninhalt und Niveau:	Das Projekt kann in allen Teilbereichen der Informatik bearbeitet werden, hat aber in der Regel einen starken Bezug zu aktuellen Forschungsthemen der betreuenden Hochschule. Im Vordergrund stehen praktische Arbeiten im Umfeld eines laufenden Forschungsprojekts, wie z.B. Implementierungen. Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden können umfangreiche praktische Arbeiten im Umfeld wissenschaftlicher Forschungsthemen selbstständig durchführen. *Methodenkompetenz:* Die Studierenden sind in der Lage, eigenständige Projekte zu bearbeiten, Informationen zu interpretieren und zu bewerten bzw. komplexe Sachverhalte der Informatik zu erkennen. *Sozialkompetenz:* Durch die Enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können komplexe praktische Fragestellung bearbeiten und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten. Sie sind in der Lage, ihren eigenen Fortschritt zu überwachen und steuern.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	
Literatur:	

Bachelorarbeit

Modulbezeichnung:	Bachelorarbeit
Studiengang:	Bachelor IT-Sicherheit
Verwendbarkeit:	berufsbegleitender Bachelorstudiengang IT-Sicherheit
Lehrveranstaltungen und Lehrformen:	Bachelorarbeit
Modulverantwortliche(r):	Betreuender Dozent kann jeder Professor des Studiengangs sein.
Lehrende:	Betreuender Dozent kann jeder Professor des Studiengangs sein.
Dauer:	1 Semester
Credits:	15 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Ausarbeitung (Bachelorarbeit) im Umfang von 20-50 Seiten, mündliche Präsentation im Umfang von 30 Minuten und anschliessende Fachdiskussion im Umfang von 30 Minuten (Kolloquium)
Berechnung der Modulnote:	
Notwendige Voraussetzungen:	• Studienleistungen im Umfang von mindestens 120 ECTS • Proseminar
Empfohlene Voraussetzungen:	Keine
Unterrichts- und Prüfungssprache:	Deutsch oder Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik
Einordnung ins Fachsemester:	Studiensemester 9
Generelle Zielsetzung des Moduls:	
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 450 h Präsenzzeit: 1 h • Kolloquium Eigenstudium: 449 h • Themenbearbeitung • Besprechungen mit dem Betreuer • Vorbereitung der Präsentation

Lerninhalt und Niveau:	Die Bachelorarbeit kann in allen Teilbereichen der Informatik geschrieben werden. Insbesondere relevant sind die folgenden Themen: • Softwareentwicklung • IT-Sicherheit im Allgemeinen • Netz- und Systemsicherheit • Digitale Forensik • Kryptographie • Theoretische Informatik • Compilerbau • Softwareentwicklung • Algorithmen und Datenstrukturen Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden beherrschen die Grundlagen des wissenschaftlichen Arbeitens in ihrem Fachgebiet und können eine begrenzte Fragestellung auf dem Gebiet der Informatik selbstständig bearbeiten *Methodenkompetenz:* Die Studierenden sind in der Lage, Grundlegende Forschungsmethodik der Informatik anzuwenden, eigenständige Projekte zu bearbeiten, Informationen zu interpretieren und zu bewerten bzw. komplexe Sachverhalte der Naturwissenschaft zu erkennen. *Sozialkompetenz:* Durch die Enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können komplexe fachbezogene Inhalte klar und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten. Sie sind in der Lage, ihren eigenen Fortschritt zu überwachen und steuern
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	
Literatur:	