



**MODULHANDBUCH**  
**Unternehmens- und IT-Si-  
cherheit (UNITS)**  
**(UNITS-B)**

Stand: 20.04.2026

Studien- und Prüfungsordnung 20232

## Modulhandbuch UNITS-B

### Inhaltsverzeichnis

Erster Studienabschnitt.....	4
1. Semester.....	4
UNITS-01: Grundlagen der Mathematik.....	5
UNITS-02: Einführung in die IT-Security.....	7
UNITS-03: Computernetze.....	9
UNITS-04: Programmierung.....	11
UNITS-05: Quantitatives Management.....	13
2. Semester.....	15
UNITS-06: Diskrete Mathematik.....	16
UNITS-07: Kryptografie.....	16
UNITS-08: Software Engineering.....	17
UNITS-09: Scripting & Hacking.....	19
UNITS-10: Zugriffskontrolle und Betriebssysteme.....	20
UNITS-11: Wirtschaftskriminalität und Data Science.....	21
Zweiter Studienabschnitt.....	23
3. Semester.....	23
UNITS-12: Algorithmen & Datenstrukturen.....	24
UNITS-13: Interaktive verteilte Systeme.....	25
UNITS-14: Datenbanken.....	26
UNITS-15: Sicherheit & Unternehmenskultur.....	28
UNITS-16: Recht.....	30
4. Semester.....	33
UNITS-30: Sicherheit in Webapplikationen.....	34
UNITS-31: Netzwerk-Sicherheit.....	36
UNITS-32: Sicherheitsmanagement und Unternehmensprozesse.....	37
UNITS-33: Unternehmenspraxis.....	39
5. Semester.....	41
UNITS-35: Projektarbeit.....	42
6. Semester.....	44
UNITS-34: Sicherheits- und Risikomanagement.....	45
UNITS-36: Computer-Forensik.....	46
7. Semester.....	49
UNITS-66: Security Analysen & Pentesting.....	50
UNITS-37: International Security Trends.....	50
UNITS-38: Bachelorarbeit.....	52
UNITS-61: Reverse Engineering.....	53
UNITS-62: Penetration Testing.....	53
UNITS-63: Verlässliche verteilte Systeme.....	54
UNITS-64: Prävention & Krisenmanagement.....	55
UNITS-65: Red Teaming & IT Infrastruktur Sicherheit.....	56
UNITS-67: Applied Cryptanalysis.....	56

# Erster Studienabschnitt

## 1. Semester

UNITS-01: Grundlagen der Mathematik

UNITS-02: Einführung in die IT-Security

UNITS-03: Computernetze

UNITS-04: Programmierung

UNITS-05: Quantitatives Management

## UNITS-01: Grundlagen der Mathematik

Empfohlene Vorkenntnisse	Hochschulzugangsberechtigung	
Lehrform	Vorlesung/Übung	
Lernziele	<p>Aneignung von Grundkenntnissen der Linearen Algebra und Analysis für die Anwendung in den Bereichen Risikoanalyse, Rechnungswesen und den verschiedenen Security-Disziplinen im späteren Studienverlauf</p> <p>Themen:</p> <ul style="list-style-type: none"> <li>- Rechnen mit reellen Zahlen</li> <li>- Funktionen und ihre Eigenschaften</li> <li>- Differential- und Integralrechnung</li> <li>- Differentialrechnung von Funktionen mit mehreren Variablen</li> <li>- Matrizen, Determinanten, Adjunkte</li> <li>- Lineare Gleichungssystem</li> <li>- Mengenlehre</li> <li>- Logik</li> <li>- Binärzahlen</li> <li>- Kombinatorik</li> </ul>	
Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP	20% Bonuspunkte für Klausur aus bewerteten Abgaben	
Modulverantwortung	Dr. Gisela Hillenbrand	
Empfohlenes Semester	1. Semester	
Häufigkeit	jedes 2. Semester	
Verwendbarkeit	Unternehmens- und IT-Sicherheit Bachelor, 1. Studienabschnitt	

<b>LEHRVERANSTALTUNG: Grundlagen Mathematik</b>		
Art	Vorlesung/Übung	
Nr.	M+I130	
SWS	4,00 SWS	
Lerninhalt	<p>Die Studierenden können die Rechengesetze der reellen Zahlen anwenden, kennen die wichtigsten Funktionsklassen. Sie beherrschen die Differentialrechnung von Funktionen einer Variablen und deren Anwendungen und erhalten eine Einführung in die Differentialrechnung von Funktionen mit mehreren Variablen. In der linearen Algebra können die Studierenden mit Matrizen rechnen und erhalten eine Einführung in die Lösungstheorie linearer Gleichungssysteme.</p>	
Lehrveranstaltungs-sprache	de	

<b>Literatur</b>	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.
------------------	--

## UNITS-02: Einführung in die IT-Security

<b>Empfohlene Vorkenntnisse</b>	Allgemeiner Umgang mit Computern	
<b>Lehrform</b>	Vorlesung/Labor	
<b>Lernziele</b>	<ul style="list-style-type: none"> <li>- Die Vorlesung bietet eine Einführung in die Grundlagen der IT-Sicherheit, wobei die einzelnen Schwerpunkte strukturiert und in einen Gesamtzusammenhang gestellt werden. Hauptziele dabei sind:</li> <li>- einen Überblick über die wesentlichen Ziele, Konzepte und Modelle der IT-Sicherheit gewinnen</li> <li>- Mittel und Wirkungsweise von Angriffen und relevanter Schutzmaßnahmen verstehen</li> <li>- Methoden und Techniken zu Entwurf und praktischer Realisierung sicherer IT-Systeme im Grundzug kennen lernen</li> <li>-</li> <li>- Wechselwirkung der Informatik mit verschiedenen Lebensbereichen kennenlernen und einschätzen können</li> <li>-</li> <li>- Zugänge zu interdisziplinären Diskursen der Gesellschaft eröffnen</li> </ul>	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	5 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	75,00 h
	Selbststudium/Gruppenarbeit:	105,00 h
	Workload:	180,00 h
<b>ECTS</b>	7,50 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	Klausur 90 Min. (K90) und Labor (LA)	
<b>Modulverantwortung</b>	Prof. Dr. rer. nat. Daniel Hammer	
<b>Empfohlenes Semester</b>	1. Semester	
<b>Häufigkeit</b>	jedes 2. Semester	
<b>Verwendbarkeit</b>	Bachelor Unternehmens- und IT-Sicherheit, 1. Studienabschnitt	

<b>LEHRVERANSTALTUNG: Einführung in die IT-Security</b>		
<b>Art</b>	Vorlesung	
<b>Nr.</b>	M+I131	
<b>SWS</b>	2,00 SWS	
<b>Lerninhalt</b>	<ul style="list-style-type: none"> <li>- Internet-Attacken im Wandel der Zeit, verändertes Sicherheitsumfeld durch zunehmende Vernetzung und die Entwicklung einer neuen Online-Medienkultur</li> <li>- Identifikation, Authentisierung und Autorisierung</li> <li>- Methoden der vertraulichen Kommunikation in modernen Medien, Einwegfunktionen, digitale Signaturen, linguistische und technische Ansätze der Steganographie und deren praktische Realisierung, versteckte Informationen in Audio- und Videodokumenten</li> <li>- Vorbereitung, Durchführung und Abwehr von Angriffen auf Kommunikationsdienste, sichere Wege in Netzen, Firewalls, und</li> </ul>	

	Angreiferwarnsysteme; Spam, Phishing und anderer eMail-Missbrauch, Abwehrstrategien u.a. mit RBL, DUL, heuristischen Methoden, Greylisting und deren rechtliche Tücken - Ethische Grundlagen - Probleme und Spannungsfelder der Medienethik, Besondere Probleme der Informatik
Lehrveranstaltungs-sprache	de
Literatur	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

<b>LEHRVERANSTALTUNG: Praktikum IT-Security</b>	
Art	Labor/Studio
Nr.	M+I132
SWS	1,00 SWS
Lerninhalt	
Lehrveranstaltungs-sprache	de
Literatur	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

<b>LEHRVERANSTALTUNG: Informatik &amp; Ethik</b>	
Art	Vorlesung
Nr.	M+I133
SWS	2,00 SWS
Lerninhalt	- Grundlagen der Ethik - Anwendungen in der IT: Privacy, Intellectual Property, Hacking - Grundbegriffe der Spieltheorie
Lehrveranstaltungs-sprache	de
Literatur	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

## UNITS-03: Computernetze

Empfohlene Vorkenntnisse	keine	
Lehrform	Vorlesung/Labor	
Lernziele	Den Aufbau und die Funktionsweise von Computernetzen verstehen; die Kommunikation über das Internet mit den bekannten Protokollen (z.B. IP, TCP, UDP, DNS, DHCP etc.) und Algorithmen verstehen und bewerten können; in der Praxis Netzwerke konfigurieren und verwalten können; aktuelle Entwicklungen im Internet analysieren und kritisch bewerten können.	
Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP	Klausur 60 Min. (K60) und Labor (LA)	
Modulverantwortung	Prof. Dr. C. Schmidt	
Empfohlenes Semester	1. Semester	
Häufigkeit	jedes Semester	
Verwendbarkeit	Bachelor Unternehmens- und IT-Sicherheit, 1. Studienabschnitt Medien und Informationswesen, 2. Studienabschnitt Medientechnik Wirtschaft+, 2. Studienabschnitt	

LEHRVERANSTALTUNG: Computernetze	
Art	Vorlesung
Nr.	M+I217
SWS	3,00 SWS
Lerninhalt	<ul style="list-style-type: none"> <li>- Grundlagen Computernetze</li> <li>- Lokale Netzwerke</li> <li>- IP - das Internet Protocol und Routing im Internet</li> <li>- Transportprotokolle im Internet (TCP, UDP und RTP)</li> <li>- Ausgewählte Anwendungen (Voice over IP, Multimediale Kommunikation, Domain Name Service, etc.)</li> </ul>
Lehrveranstaltungs-sprache	de
Literatur	Eine aktuelle Literaturliste wird in der Vorlesung bekanntgegeben.

LEHRVERANSTALTUNG: Labor Computernetze	
Art	Labor
Nr.	M+I218
SWS	1,00 SWS

<b>Lerninhalt</b>	<ul style="list-style-type: none"> <li>- Konfiguration des Netzwerkzugangs und von Router, Switches und NAT-Gateways</li> <li>- Netzwerkkommandos zur Analyse und Konfiguration</li> <li>- Netzwerkanalyse mit Wireshark</li> <li>- LAN- und Internetprotokolle im praktischen Einsatz</li> </ul>
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	Eine aktuelle Literaturliste wird in der Veranstaltung bekanntgegeben.

## UNITS-04: Programmierung

Empfohlene Vorkenntnisse	keine	
Lehrform	Vorlesung/Labor	
Lernziele	&#9679; Prozedurale Programmieretechniken, sowie erste Objektorientierte Konzepte verstehen und in der Programmiersprache C anwenden können &#9679; Strukturiertes und sicheres Programmieren in C	
Dauer	1 Semester Semester	
SWS	6 SWS	
Aufwand	Lehrveranstaltung:	90,00 h
	Selbststudium/Gruppenarbeit:	180,00 h
	Workload:	270,00 h
ECTS	7,50 ECTS	
Voraussetzungen für die Vergabe von LP	Klausurarbeit, 90 Min. und Laborarbeit (Sprachgrundlagen und wichtige Programmieretechniken zu prozeduraler Programmierung in C sowie erste Konzepte objektorientierter Programmierung, Labor zu prozeduraler bzw. objektorientierter Programmierung in C mit einem Augenmerk auf 'sicherer' Programmierung.)	
Modulverantwortung	Prof. Dr. Dirk Westhoff	
Empfohlenes Semester	1. Semester	
Häufigkeit	jedes 2. Semester	
Verwendbarkeit	Bachelor Unternehmens- und IT-Sicherheit, 1. Studienabschnitt	

<b>LEHRVERANSTALTUNG: Programmierung</b>	
Art	Vorlesung
Nr.	M+I370
SWS	4,00 SWS
Lerninhalt	<ul style="list-style-type: none"> <li>- Einführung in die prozedurale Programmierung in C / C++</li> <li>- Datentypen</li> <li>- Kontrollstrukturen</li> <li>- Funktionen</li> <li>- Zeiger</li> <li>- Datenstrukturen</li> <li>- Aufbau des Speichers</li> <li>- Objektorientierung mit C++</li> <li>- Sichere Programmierung</li> </ul>
Lehrveranstaltungs-sprache	de
Literatur	Goll / Dausmann "Einführung in C", Springer Vieweg, 8. Auflage, 2014 Küveler / Schwoch "C / C++ für STudium und Beruf", Springer Vieweg, 2017

<b>LEHRVERANSTALTUNG: Labor Programmierung</b>
--

Art	Labor
Nr.	M+I371
SWS	2,00 SWS
Lerninhalt	Einführung in C/C++, IDEs, Gitlab Übungen zu prozeduraler Programmierung Übungen zu objektorientierter Programmierung
Lehrveranstaltungs- sprache	de
Literatur	

## UNITS-05: Quantitatives Management

<b>Empfohlene Vorkenntnisse</b>	Grundkenntnisse der Mathematik und Statistik erworben durch die Hochschulzugangsberechtigung	
<b>Lehrform</b>	Vorlesung	
<b>Lernziele</b>	Lernziel 1: Die Studierenden sollen Fakten und Informationen bezüglich der quantitativen Methoden aufnehmen und wiedergeben können. Lernziel 2: Die Studierenden sollen ein Verständnis bezüglich der quantitativen Methoden entwickeln, um Informationen erläutern zu können. Lernziel 3: Die Studierenden sollen die Techniken der quantitativen Methoden in veränderten und neuen Kontexten anwenden können.	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	4 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
<b>ECTS</b>	5,00 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	Klausur 90Min (K90)	
<b>Modulverantwortung</b>	Prof. Dr. Dirk Drechsler	
<b>Empfohlenes Semester</b>	1. Semester	
<b>Häufigkeit</b>	jedes 2. Semester	
<b>Verwendbarkeit</b>	Unternehmens- und IT-Sicherheit Bachelor, 1. Studienabschnitt	

<b>LEHRVERANSTALTUNG: Statistische Methoden der Unternehmensanalyse 1</b>	
<b>Art</b>	Vorlesung
<b>Nr.</b>	M+I394
<b>SWS</b>	4,00 SWS
<b>Lerninhalt</b>	A. Deskriptive Statistik - Empirische Verteilungen - Lage- und Streuungsparameter - Quartile und Boxplot - Beschreibung von Populationen - Bivariate Deskriptive Statistik B. Wahrscheinlichkeitstheorie - Mengenlehre - Abzähltechniken - Grundlagen der Wahrscheinlichkeitsrechnung - Bedingte Wahrscheinlichkeit und Unabhängigkeit - Zufallsvariablen - Statistische Verteilungen

	<p>C. Wahrscheinlichkeitsverteilungen</p> <ul style="list-style-type: none"> <li>- Diskrete Verteilungen</li> <li>- Stetige Verteilungen</li> </ul>
<b>Lehrveranstaltungs- sprache</b>	de
<b>Literatur</b>	<p>Empfohlene Literatur:</p> <ul style="list-style-type: none"> <li>- Bley Müller, J. et al. (2020): Statistik für Wirtschaftswissenschaftler; 18. Auflage; Vahlen.</li> <li>- Lipschutz, S.; Lipson, M. (2011): Probability; 2. Auflage; McGraw Hill.</li> <li>- Spiegel, M.R.; Stephens, L.J. (2018): Statistics; 6. Auflage; McGraw Hill.</li> </ul>

## 2. Semester

UNITS-06: Diskrete Mathematik

UNITS-07: Kryptografie

UNITS-08: Software Engineering

UNITS-09: Scripting & Hacking

UNITS-10: Zugriffskontrolle und Betriebssysteme

UNITS-11: Wirtschaftskriminalität und Data Science

## UNITS-06: Diskrete Mathematik

Empfohlene Vorkenntnisse	keine erforderlich
Lehrform	Labor
Lernziele	Die Studierenden haben die mathematischen Grundlagen verstanden, die der Kryptografie und der Algorithmik zugrundeliegen, und können diese in dem Zusammenhang sicher anwenden. Themen: - Modulares Rechnen - Codierungstheorie - Diskrete Optimierung - Gruppen, Ringe, Körper
Dauer	1 Semester
SWS	4 SWS
Aufwand	Lehrveranstaltung: 60,00 h
	Selbststudium/Gruppenarbeit: 90,00 h
	Workload: 150,00 h
ECTS	5,00 ECTS
Voraussetzungen für die Vergabe von LP	Benotete Laborabgaben
Modulverantwortung	Prof. Dr. Gisela Hillenbrand
Empfohlenes Semester	2. Semester
Häufigkeit	jedes Jahr (SS)
Verwendbarkeit	Unternehmens- und IT-Sicherheit Bachelor, 1. Studienabschnitt

<b>LEHRVERANSTALTUNG: Diskrete Mathematik</b>	
Art	Labor
Nr.	M+I139
SWS	4,00 SWS
Lerninhalt	- Einführung in algebraische Strukturen und deren Rechengesetze - Modulares Rechnen und Anwendungen - Einführung in die Codierungstheorie - Einführung in die Graphentheorie und deren Anwendung in der Diskreten Optimierung
Lehrveranstaltungs-sprache	de
Literatur	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

## UNITS-07: Kryptografie

Empfohlene Vorkenntnisse	Kenntnisse einer Sprache wie C/C++, Java oder Python
Lehrform	Labor

<b>Lernziele</b>	Die Studierenden kennen und verstehen den Prozess und die Methodik der systematischen Software-Entwicklung und sie können diese Kenntnisse für konkrete Aufgabenstellungen einsetzen.
<b>Dauer</b>	1 Semester
<b>SWS</b>	4 SWS
<b>Aufwand</b>	Lehrveranstaltung: 45,00 h
	Selbststudium/Gruppenarbeit: 105,00 h
	Workload: 150,00 h
<b>ECTS</b>	5,00 ECTS
<b>Voraussetzungen für die Vergabe von LP</b>	
<b>Modulverantwortung</b>	Prof. Dr. Erik Zenner
<b>Empfohlenes Semester</b>	2. Semester
<b>Häufigkeit</b>	jedes Jahr (SS)
<b>Verwendbarkeit</b>	Unternehmens- und IT- Sicherheit, 1. Studienabschnitt

<b>LEHRVERANSTALTUNG: Grundlagen der Kryptografie</b>	
<b>Art</b>	Labor
<b>Nr.</b>	M+I140
<b>SWS</b>	4,00 SWS
<b>Lerninhalt</b>	<ul style="list-style-type: none"> <li>- Grundbegriffe (Rolle im Gesamtkonzept der IT-Sicherheit, Schlüssel und Algorithmus, Modellierung kryptographischer Probleme)</li> <li>- Verschlüsselung (Schutzziel Vertraulichkeit, historische Chiffren, Blockchiffren, Stromchiffren)</li> <li>- Authentifizierung (Schutzziel Authentifizierung, Hashfunktionen, MACs)</li> <li>- Schlüsselverwaltung (Schlüsselerzeugung, Aushandeln und Übertragen von Schlüsseln, Post-Quantum-Kryptographie)</li> <li>- Digitale Signatur (Schutzziel Unablegbarkeit, Signaturverfahren, Public-Key-Infrastrukturen)</li> </ul>
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	<ul style="list-style-type: none"> <li>- Niels Ferguson, Bruce Schneier, Tadayoshi Kohno: Cryptography Engineering (Wiley, 2010)</li> <li>- Christof Paar, Jan Pelzl: Kryptografie verständlich (Springer vieweg, 2016)</li> </ul>

## UNITS-08: Software Engineering

<b>Empfohlene Vorkenntnisse</b>	Grundlagen der prozeduralen Programmierung IT Grundlagen
<b>Lehrform</b>	Vorlesung/Übung
<b>Lernziele</b>	Die / Der Studierende soll lernen wie kontrolliert auf Basis von definierten Policies auf Objekte in Systemen zugegriffen werden kann (Zugriffskontrollsysteme). Auch soll vermittelt werden wie Aufgaben in Linux / Windows

	Umgebungen automatisiert werden können (Scripting & Hacking) und erste IT Sicherheitsprobleme mit Python gelöst werden. Der grundlegende Aufbau von Python 3 wird vermittelt.	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	4 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	90,00 h
	Selbststudium/Gruppenarbeit:	150,00 h
	Workload:	240,00 h
<b>ECTS</b>	5,00 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	Hausarbeit (HA)	
<b>Modulverantwortung</b>	Prof. Dr. Andreas Schaad	
<b>Empfohlenes Semester</b>	2. Semester	
<b>Häufigkeit</b>	jedes Jahr (SS)	
<b>Verwendbarkeit</b>	Unternehmens- und IT-Sicherheit Bachelor, 1.Studienabschnitt	

<b>LEHRVERANSTALTUNG: Software Engineering (UN)</b>	
<b>Art</b>	Vorlesung/Übung
<b>Nr.</b>	M+I122
<b>SWS</b>	4,00 SWS
<b>Lerninhalt</b>	Lecture 1: Basic History of the Software Engineering Discipline Lecture 2: Requirements Engineering Lecture 3/4: UML-based Design Lecture 5: Coding - Best Practices Lecture 6: Testing Software Lecture 7: Different Development Approaches Lecture 8: Motivating a secure Development Lifecycle Lecture 9: Secure Programming Lecture 10: Static Code Analysis Lecture 11: CVSS-based Vulnerability Analysis Lecture 12: Selected reading of very recent (and very old "test of time") papers
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	Sommerville, I. "Software Engineering (10th Edition)" Martin, R. "Clean Code" Martin, R. "Clean Architecture" Brooks, F. "The Mythical Man-Month: Essays on Software Engineering" Fowler, M. "UML Distilled" <a href="https://mi&amp;#8208;learning.mi.hs&amp;#8208;offenburg.de/SWE/">https://mi&amp;#8208;learning.mi.hs&amp;#8208;offenburg.de/SWE/</a> (in German) Any material mentioned in the lecture (e.g. Online Secure Coding Guidelines for C/C++)

## UNITS-09: Scripting & Hacking

Empfohlene Vorkenntnisse	Hochschulzugangsberechtigung, Erfahrungen im Umgang mit Rechnern	
Lehrform	Vorlesung/Übung	
Lernziele	Die Studierenden... - verstehen Aufbau und Arbeitsweise von Computersystemen - kennen die wichtigsten Bestandteile, Aufgaben und Funktionen eines Betriebssystems - verstehen das Zusammenwirken der verschiedenen Komponenten sowie der dabei verwendeten technischen Methoden und praktischen Verfahren	
Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	60,00 h
	Workload:	120,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP	Hausarbeit (HA)	
Modulverantwortung	Prof. Dr. Andreas Schaad	
Empfohlenes Semester	2. Semester	
Häufigkeit	jedes Jahr (SS)	
Verwendbarkeit	Unternehmens und IT-Sicherheit, 1. Studienabschnitt	

LEHRVERANSTALTUNG: Skripting & Hacking	
Art	Vorlesung/Übung
Nr.	M+I372
SWS	4,00 SWS
Lerninhalt	Dem Studierenden sollen erste Kenntnisse der SHELL Programmierung vermittelt werden (25%): - Klassische UNIX Shell - Klassische Windows CMD - Windows Powershell - erste Capture the Flag Aufgaben (OTW) Ferner sollen primär erste Kenntnisse der Python Programmierung vermittelt werden (75%): - Fokus ist auf grundlegenden Datentypen und Kontrollstrukturen - Reguläre Ausdrücke - Objektorientierung - Interaktion mit Betriebs- und Dateisystem - Netzwerkprogrammierung - (Vereinfachte) Beispiele und Szenarien aus der IT Sicherheit KEIN Ziel dieser Vorlesung sind push-button Umgebungen wie KALI Linux etc.
Lehrveranstaltungs-sprache	de

<b>Literatur</b>	<p>"Python 3 Das umfassende Handbuch" von Johannes Ernesti, Peter Kaiser, Rheinwerk Verlag, 2017</p> <p>"Python Hacking", TJ. O Connor, FRANZIS Verlag GmbH; Auflage: 1 (28. September 2015)</p> <p>"Mehr Hacking mit Python: Eigene Tools entwickeln für Hacker und Pentester" Justin Seitzd, punkt.verlag GmbH; 1., Auflage (17. September 2015)</p> <p>"Shell-Programmierung: Das umfassende Handbuch. Für Bourne-, Korn- und Bourne-Again-Shell (bash)" Jürgen Wolf, Rheinwerk Computing; Auflage: 5 (29. März 2016)</p>
------------------	--

## UNITS-10: Zugriffskontrolle und Betriebssysteme

<b>Empfohlene Vorkenntnisse</b>	Keine
<b>Lehrform</b>	Vorlesung/Labor
<b>Lernziele</b>	<p>Die Studierenden können nach Abschluss des Moduls</p> <ul style="list-style-type: none"> <li>- ...Fakten, Wissen und Konzepte erlernen in Bezug auf Wirtschafts- und Cyberkriminalität sowie Buchhaltung und Kostenrechnung,</li> <li>- ...Kernideen der Vorlesungen in Bezug auf Wirtschafts- und Cyberkriminalität sowie Buchhaltung und Kostenrechnung verstehen, für sich organisieren, interpretieren und selbständig beschreiben,</li> <li>- ...das erworbene Wissen in Bezug auf Wirtschafts- und Cyberkriminalität sowie Buchhaltung und Kostenrechnung in neuen Situationen für eine Problemlösung heranziehen,</li> <li>- ...komplexere Sachverhalte in Bezug auf Wirtschafts- und Cyberkriminalität sowie Buchhaltung und Kostenrechnung aufbrechen, um neues anwendungsbezogenes Wissen zu generieren.</li> </ul>
<b>Dauer</b>	1 Semester
<b>SWS</b>	4 SWS
<b>Aufwand</b>	Lehrveranstaltung: 60,00 h
	Selbststudium/Gruppenarbeit: 90,00 h
	Workload: 150,00 h
<b>ECTS</b>	5,00 ECTS
<b>Voraussetzungen für die Vergabe von LP</b>	Modulklausur (K60 - 60 Minuten) + Laborarbeit (LA)
<b>Modulverantwortung</b>	Prof. Dr. Daniel Hammer
<b>Empfohlenes Semester</b>	2. Semester
<b>Häufigkeit</b>	jedes Jahr (SS)
<b>Verwendbarkeit</b>	<p>Bachelor Unternehmens- und IT-Sicherheit, 1. Studienabschnitt (UNITS)</p> <p>Betriebliches Rechnungswesen</p> <p>Bachelor Medien und Informationswesen (MI)</p> <p>Occupational Fraud</p>

<b>LEHRVERANSTALTUNG: Zugriffskontrolle und Betriebssysteme</b>	
<b>Art</b>	Vorlesung

Nr.	M+I382
SWS	3,00 SWS
Lerninhalt	
Lehrveranstaltungs- sprache	de
Literatur	

<b>LEHRVERANSTALTUNG: Labor Zugriffskontrolle und Betriebs- systeme</b>	
Art	Labor
Nr.	M+I383
SWS	0,00 SWS
Lerninhalt	
Lehrveranstaltungs- sprache	de
Literatur	

## UNITS-11: Wirtschaftskriminalität und Data Science

Empfohlene Vorkenntnisse	Modul-05 Quantitative Management	
Lehrform	Vorlesung	
Lernziele	Die Studierenden sollten - den Nutzen quantitativer Methoden im Rahmen der Unternehmens- und IT-Sicherheit verstehen, - die Methoden im Rahmen kontrollierter Aufgabenstellungen anwenden und - erste eigene Auswertungen eigenständig berechnen können.	
Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	90,00 h
	Selbststudium/Gruppenarbeit:	150,00 h
	Workload:	240,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP	Klausur K90	
Modulverantwortung	Prof. Dr. Dirk Drechsler	
Empfohlenes Semester	2. Semester	
Häufigkeit	jedes 2. Semester	
Verwendbarkeit	Unternehmens- und IT-Sicherheit Bachelor, 1. Studienabschnitt	

<b>LEHRVERANSTALTUNG: Occupational Fraud</b>	
Art	Vorlesung

Nr.	M+I178
SWS	2,00 SWS
Lerninhalt	I. Gesellschaftliche Entwicklungen II. Neue Aspekte der menschlichen Interaktion III. Persönlichkeitsstörungen und Wirtschaftskriminalität IV. Theorien zum Verständnis von Kriminalität V. Formen von Cyberbedrohungen VI. Profile von Cyberkriminellen
Lehrveranstaltungs-sprache	de
Literatur	Albrecht, W.S./Albrecht, C.O./Albrecht, C.C./Zimbelman, M.F.; Fraud Examination; Cengage Learning; aktuelle Auflage. Lamnek, S.; Theorien abweichenden Verhaltens I, "Klassische" Ansätze; UTB; aktuelle Auflage. Lamnek, S.; Theorien abweichenden Verhaltens II, "Moderne" Ansätze; UTB; aktuelle Auflage. Pontell, H.N./Geis, G.; International Handbook of White-Collar Crime; Springer; aktuelle Auflage. Wells, J.T./Kopetzky, M.; Handbuch Wirtschaftskriminalität; LexisNexis; aktuelle Ausgabe.

<b>LEHRVERANSTALTUNG: Statistische Methoden der Unternehmensanalyse 2</b>	
Art	Vorlesung
Nr.	M+I395
SWS	2,00 SWS
Lerninhalt	Kap. A Einleitung Kap. B Schätzungen und Hypothesen Kap. C Stochastische Prozesse Kap. D Entscheidungsanalyse
Lehrveranstaltungs-sprache	de
Literatur	Albright, S.C./Winston, W.L.; Business Analytics, Data and Decision Making; Cengage; Actual Edition. Anderson, D.R./Sweeney, D.J./Williams, T.A./Camm, J.D./Cochran, J.J./Fry, M.J./Ohlmann, J.W.; Quantitative Methods for Business; Cengage; Actual Edition. Berenson, M.L./Levine, D.M./Krehbiel, T.C.; Basic Business Statistics; Pearson; Actual Edition.

# Zweiter Studienabschnitt

## 3. Semester

UNITS-12: Algorithmen & Datenstrukturen

UNITS-13: Interaktive verteilte Systeme

UNITS-14: Datenbanken

UNITS-15: Sicherheit & Unternehmenskultur

UNITS-16: Recht

## UNITS-12: Algorithmen & Datenstrukturen

<b>Empfohlene Vorkenntnisse</b>	- Webseiten in HTML5 beschreiben können - prozedural programmieren können	
<b>Lehrform</b>	Vorlesung/Labor	
<b>Lernziele</b>	- die Bedeutung von User Interfaces und Rechnernetzen für interaktive verteilte Systeme erkennen - das Internet als weltweite Infrastruktur sowie seine Dienste verstehen, gegeneinander abwägen und einsetzen - das World Wide Web als interaktives verteiltes System erkennen sowie Web-Technologien verstehen und einsetzen - Anwendungen als bestimmenden Faktor des Internet erkennen und über neue Anwendungen nachdenken TEST, TEST	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	6 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
<b>ECTS</b>	8,00 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	Klausurarbeit, 60 Min. und Laborarbeit (Interaktive verteilte Systeme, Labor Interaktive verteilte Systeme)	
<b>Modulverantwortung</b>	Prof. Dr. Erik Zenner	
<b>Empfohlenes Semester</b>	3. Semester	
<b>Häufigkeit</b>	jedes 2. Semester	
<b>Verwendbarkeit</b>	Bachelor Unternehmens- und IT-Sicherheit, 2. Studienabschnitt	

<b>LEHRVERANSTALTUNG: Algorithmen &amp; Datenstrukturen</b>	
<b>Art</b>	Vorlesung
<b>Nr.</b>	M+I145
<b>SWS</b>	4,00 SWS
<b>Lerninhalt</b>	- Grundbegriffe, Komplexitätsrechnung - Rekursion - Elementare Datenstrukturen - Hashtabellen - Sortierverfahren - Bäume und Graphen - Greedy-Algorithmen - Backtracking - Time-Memory-Tradeoffs - Heuristiken
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

<b>LEHRVERANSTALTUNG: Labor Algorithmen &amp; Datenstrukturen</b>	
Art	Labor/Studio
Nr.	M+I146
SWS	2,00 SWS
Lerninhalt	- Vertiefen von Programmierkenntnissen - Anwendung von algorithmischen Techniken auf konkrete Problemstellungen
Lehrveranstaltungs-sprache	de
Literatur	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

## UNITS-13: Interaktive verteilte Systeme

Empfohlene Vorkenntnisse	Kenntnisse einer Programmiersprache	
Lehrform	Vorlesung/Labor	
Lernziele	- Die Studierenden können Konzepte für die effiziente, strukturierte Datenverwaltung in der Praxis anwenden - Sie verstehen die Bedeutung der Datenhaltung in unserer Welt und können diese einordnen und bewerten	
Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP	Klausur 60 Min. + Laborarbeit (K60 + LA)	
Modulverantwortung	Prof. Dr. Tom Rüdebusch	
Empfohlenes Semester	3. Semester	
Häufigkeit	jedes 2. Semester	
Verwendbarkeit	Bachelor Unternehmens- und IT-Sicherheit, 1. Studienabschnitt	

<b>LEHRVERANSTALTUNG: Interaktive verteilte Systeme</b>	
Art	Vorlesung
Nr.	M+I219
SWS	3,00 SWS
Lerninhalt	Die LV gliedert sich folgendermaßen: - Dienste im Internet - die Systemarchitektur des World Wide Web - das Protokoll http - serverseitige Programmierung: CGI/C, PHP

	<ul style="list-style-type: none"> <li>- clientseitige Programmierung: HTML, CSS, JavaScript</li> <li>- Strukturierung von Informationen mit XML</li> <li>- Anwendungen</li> </ul>
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	<ul style="list-style-type: none"> <li>- Shneiderman et al.: Designing the User Interface. Pearson, 2017</li> <li>- Freeman: The Definitive Guide to HTML5. Apress, 2011</li> <li>- Flanagan: JavaScript. O'Reilly, 2011</li> <li>- Tatroe, MacIntyre, Lerdorf: Programming PHP. O'Reilly, 2013</li> <li>- Harold, Means: XML in a Nutshell. O'Reilly, 2004</li> </ul>

<b>LEHRVERANSTALTUNG: Labor Interaktive verteilte Systeme</b>	
<b>Art</b>	Labor
<b>Nr.</b>	M+I220
<b>SWS</b>	1,00 SWS
<b>Lerninhalt</b>	<ul style="list-style-type: none"> <li>- Web-Entwicklung auf dem Raspberry Pi</li> <li>- Internet der Dinge mit Arduino</li> <li>- Web-Anwendungen als verteiltes System</li> </ul>
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	<ul style="list-style-type: none"> <li>- Kofler, Kühnast: Raspberry Pi. Rheinwerk Computing, 2017</li> <li>- Monk: Programming Arduino. McGraw-Hill, 2013</li> </ul>

## UNITS-14: Datenbanken

<b>Empfohlene Vorkenntnisse</b>	Grundlegende Kenntnisse der Betriebswirtschaft	
<b>Lehrform</b>	Vorlesung	
<b>Lernziele</b>	<p>Die Studierenden können nach Beendigung des Moduls</p> <ul style="list-style-type: none"> <li>- ...Fakten, Wissen und Konzepte erlernen bezüglich der unternehmerischen Strategie, Organisation, Corporate Governance, Compliance, Sicherheitsstandards und der mathematischen Statistik,</li> <li>- ...Kernideen der Vorlesungen verstehen, für sich organisieren, interpretieren und selbständig beschreiben bezüglich der unternehmerischen Strategie, Organisation, Corporate Governance, Compliance, Sicherheitsstandards und der mathematischen Statistik,</li> <li>- ...das erworbene Wissen in neuen Situationen für eine Problemlösung heranziehen bezüglich der unternehmerischen Strategie, Organisation, Corporate Governance, Compliance, Sicherheitsstandards und der mathematischen Statistik,</li> <li>- ...komplexere Sachverhalte aufbrechen, um neues anwendungsbezogenes Wissen zu generieren bezüglich der unternehmerischen Strategie, Organisation, Corporate Governance, Compliance, Sicherheitsstandards und der mathematischen Statistik.</li> </ul>	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	4 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	90,00 h

	Selbststudium/Gruppenarbeit:	120,00 h
	Workload:	210,00 h
<b>ECTS</b>	5,00 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	Modulklausur K90 (90 Minuten) - Strategie, Organisation und Unternehmenskultur (2,5 Credits) - Statistische Methoden der Unternehmensanalyse (2 Credits) - Corporate Governance, Compliance und Unternehmensethik (2,5 Credits)	
<b>Modulverantwortung</b>	Prof. Dr. Volker Sanger	
<b>Empfohlenes Semester</b>	3. Semester	
<b>Hufigkeit</b>	jedes Jahr (WS)	
<b>Verwendbarkeit</b>	Bachelor Unternehmens- und IT-Sicherheit, 1. Studienabschnitt Bachelor Medien und Informationswesen	

<b>LEHRVERANSTALTUNG: Datenbanken</b>	
<b>Art</b>	Vorlesung
<b>Nr.</b>	M+I223
<b>SWS</b>	3,00 SWS
<b>Lerninhalt</b>	<ul style="list-style-type: none"> <li>- Einfuhung: Datenbanksystem, Datenmodell, Datenbankanwendungen</li> <li>- Das relationale Datenmodell: Relationen und Attribute, relationale Algebra, Selektion, Join, Projektion</li> <li>- SQL: Schemadefinition, Anfragen, nderungen der Datenbasis, Views, Konsistenzbedingungen, ACID-Prinzip, SQL-Transaktionen,</li> <li>- Datenbankentwurf: Entwurfsphasen, semantische Datenmodelle, Abhangigkeiten, Normalisierung, Umsetzung semantischer Modelle in ein logisches Modell</li> <li>- Datenbank-Programmierung: JSP, Objekt-relationales Mapping, JDBC, Stored-Procedures, Trigger</li> <li>- Objektorientierte und Objektrelationale Datenbanken: Einschrankungen des relationalen Modells, ODMG-Standard, Objektmodell, ODL, OQL, SQL-3</li> <li>- No-SQL-Datenbanken, CAP und BASE</li> </ul>
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	<ul style="list-style-type: none"> <li>- A. Kemper, A. Eickler: Datenbanksysteme - Eine Einfuhung, 7. Auflage, Oldenbourg-Verlag, 2009</li> <li>- A. Heuer, G. Saake: Datenbanken: Konzepte und Sprachen, mitp-Verlag, 2008</li> <li>- R. Elmasri, S.B. Navathe: Fundamentals of Database Systems, Addison-Wesley, 2009</li> <li>- P. Gultzan, T. Pelzer: SQL-99 Complete, Really, Miller Freeman, 1999</li> <li>- M. Schubert: Datenbanken, Theorie, Entwurf und Programmierung relationaler Datenbanken, Springer-Verlag, 2007 (Im OPAC der Hochschule als e-book)</li> <li>- L. Piepmeyer: Grundkurs Datenbanksysteme &amp;ndash; Von den Konzepten bis zur Anwendungsentwicklung, Hanser-Verlag, 2011 (Im OPAC der Hochschule als e-book)</li> </ul>

<b>LEHRVERANSTALTUNG: Labor Datenbanken</b>	
Art	Labor
Nr.	M+I224
SWS	1,00 SWS
Lerninhalt	- SQL: Tabellenanlage und Datenmanipulation - Datenbanken im WWW mit JSP - Kleinprojekt: Entwicklung einer Web-Applikation mit darunter liegender Datenbank
Lehrveranstaltungs- sprache	de
Literatur	- A. Heuer, G. Saake: Datenbanken: Konzepte und Sprachen, mitp-Verlag, 2008 - R. Elmasri, S.B. Navathe: Fundamentals of Database Systems, Addison-Wesley, 2009 - A. Kemper, A. Eickler: Datenbanksysteme - Eine Einführung, Oldenbourg-Verlag, 2009

## UNITS-15: Sicherheit & Unternehmenskultur

Empfohlene Vorkenntnisse	Modul UNITS-05 Quantitatives Management	
Lehrform	Vorlesung	
Lernziele	<p>Lernziel 1: Die Studierenden sollen Fakten und Informationen bezüglich der Unternehmensstrategie/Organisation/Unternehmenskultur, der Corporate Governance/Compliance/Unternehmensethik und des betrieblichen Rechnungswesens aufnehmen und wiedergeben können.</p> <p>Lernziel 2: Die Studierenden sollen ein Verständnis bezüglich der Unternehmensstrategie/Organisation/Unternehmenskultur, der Corporate Governance/Compliance/Unternehmensethik und des betrieblichen Rechnungswesens entwickeln, um Informationen erläutern zu können.</p> <p>Lernziel 3: Die Studierenden sollen die Techniken der Unternehmensstrategie/Organisation/Unternehmenskultur, der Corporate Governance/Compliance/Unternehmensethik und des betrieblichen Rechnungswesens in veränderten und neuen Kontexten anwenden können.</p>	
Dauer	1 Semester	
SWS	6 SWS	
Aufwand	Lehrveranstaltung:	90,00 h
	Selbststudium/Gruppenarbeit:	120,00 h
	Workload:	210,00 h

ECTS	7,00 ECTS
Voraussetzungen für die Vergabe von LP	Klausur 90Min (K90)
Modulverantwortung	Prof. Dr. Dirk Drechsler
Empfohlenes Semester	3. Semester
Häufigkeit	jedes Jahr (WS)
Verwendbarkeit	Unternehmens- und IT-Sicherheit/muk Bachelor, 2. Studienabschnitt

<b>LEHRVERANSTALTUNG: Betriebliches Rechnungswesen</b>	
Art	Vorlesung
Nr.	M+I110
SWS	2,00 SWS
Lerninhalt	<ul style="list-style-type: none"> <li>- Begriffe des betrieblichen Rechnungswesens</li> <li>- Gesetzliche Bestimmungen</li> <li>- Buchführung und Buchungssätze</li> <li>- Kosten- und Leistungsrechnung</li> <li>- Gewinn- und Verlustrechnung</li> <li>- Bilanz, Bilanzveränderung und Bilanzanalyse</li> </ul>
Lehrveranstaltungs-sprache	de
Literatur	<ul style="list-style-type: none"> <li>- Schildbach / Homburg, Kosten und Leistungsrechnung, Ochsenfurt-Hohestadt, 2009</li> <li>- Andres / Köhl / Pilz, Grundlagen des Rechnungswesens, Haan-Gruiten, 2003</li> <li>- Schöttler / Spulak, Technik des betrieblichen Rechnungswesens, Oldenburg, 2003</li> <li>- Andres / Droll / Köhl / Koschar / Zoller, Rechnungswesen der Unternehmung, Haan-Gruiten, 20</li> </ul>

<b>LEHRVERANSTALTUNG: Strategie, Organisation und Unternehmenskultur</b>	
Art	Vorlesung
Nr.	M+I375
SWS	2,00 SWS
Lerninhalt	<ul style="list-style-type: none"> <li>A. Wozu diese Vorlesung???</li> <li>B. Strategische und Cyber Intelligence</li> <li>C. Digitale Ökonomien, Ökosysteme und Geschäftsmodelle</li> <li>D. Strategie und Internationalität der Unternehmung</li> <li>E. Business Information Systems (BIS) aus der Management-Perspektive</li> </ul>
Lehrveranstaltungs-sprache	de
Literatur	<ul style="list-style-type: none"> <li>Beynon-Davies, Paul; Business Information Systems; 2nd Edition; Palgrave MacMillan; Basingstoke; 2019.</li> <li>Clark, Tim et al.; Business Model You: A One-Page Method For Reinventing Your Career; John Wiley &amp; Sons; Hoboken, New Jersey; 2012.</li> <li>Goldin, Ian; Kutarna, Chris; Age of Discovery, Navigating the risks and</li> </ul>

	rewards of our new renaissance; St. Martin's Press; New York; 2016. Skilton, Mark; Building Digital Ecosystem Architectures, A Guide to Enterprise Architecting Digital Technologies in the Digital Enterprise; Palgrave McMillan; Basingstoke; 2016.
--	--

<b>LEHRVERANSTALTUNG: Corporate Governance, Compliance und Unternehmensethik</b>	
<b>Art</b>	Vorlesung
<b>Nr.</b>	M+I377
<b>SWS</b>	2,00 SWS
<b>Lerninhalt</b>	A. Wozu das Ganze? B. Wirtschafts- und Unternehmensethik C. Corporate Governance D. Compliance Management System E. Grundlagen der Informationssicherheit F. Das BSI-Modell zur Informationssicherheit G. COBIT 5.0 - IT-Governance
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	Aras, Güler; Crowther, David; Governance and Social Responsibility, International Perspectives; Palgrave 2012. BSI (Hrsg.); BSI-Standard 200-1: Managementsysteme für Informationssicherheit BSI (Hrsg.); BSI-Standard 200-2: IT-Grundschutz-Methodik COSO (Hrsg.); Fraud Risk Management; COSO; 2016. Desjardins, Joseph R.; McCall, John J.; Contemporary Issues in Business Ethics; Sixth Edition; Cengage; 2014. Freidank, Carl-Christian; Unternehmensüberwachung, Die Grundlagen betriebswirtschaftlicher Kontrolle, Prüfung und Aufsicht; Vahlen; 2012. ISACA (Ed.); COBIT 2019 Framework: Introduction and Methodology; ISACA; 2019. Mellahi, Kamel et al.; The Ethical Business, Challenges and Controversies; Second Edition; Palgrave 2010. Morrison, Janet; Business Ethics, New Challenges in a Globalized World; Palgrave, 2015. Oyevaar, Martin et al.; Globalization & Sustainable Development, A Business Perspective; Palgrave; 2016. Welge, Martin K; Eulerich, Marc; CorporateGovernance-Management, Theorie und Praxis der guten Unternehmensführung; 2. Auflage; Springer Gabler; 2014.

## UNITS-16: Recht

<b>Empfohlene Vorkenntnisse</b>	
<b>Lehrform</b>	Vorlesung
<b>Lernziele</b>	

Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP		
Modulverantwortung		
Empfohlenes Semester	3. Semester	
Häufigkeit	jedes Jahr (WS)	
Verwendbarkeit		

<b>LEHRVERANSTALTUNG: Medienrecht</b>	
Art	Vorlesung
Nr.	M+I119
SWS	2,00 SWS
Lerninhalt	<p>Die Veranstaltung führt ein in das Rechtssystem, das Recht und seine Durchsetzung, die Mediengrundrechte, die Stellung des Medienrechts und des Medienwirtschaftsrechts, die Grundlagen des Urheberrechts, die Grundfragen zu Persönlichkeitsrechten inkl. Presse- und Rundfunkrecht, die Grundlagen des Werberechts, Markenrechts, Online-Vertragsrechts inkl. AGB-Recht, Arbeitsrecht mit Medienbezug und des Datenschutzrechts.</p> <p>Einführung in das Rechtssystem, das Recht und seine Durchsetzung                      Mediengrundrechte                      Stellung des Medienrechts und des Medienwirtschaftsrechts                      Grundlagen des Urheberrechts                      Grundfragen zu Persönlichkeitsrechten inkl. Presse- und Rundfunkrecht                      Grundlagen des Werberechts                      Grundlagen des Markenrechts                      Grundlagen des Online-Vertragsrechts inkl. AGB-Recht                      Grundwissen zum Arbeitsrecht mit Medienbezug                      Grundlagen des Datenschutzrechts</p>
Lehrveranstaltungs-sprache	de
Literatur	<ul style="list-style-type: none"> <li>- Fechner, Medienrecht, 18. Aufl. 2017</li> <li>- Lettl, Wettbewerbsrecht, 3. Aufl. 2016</li> <li>- Nordemann, Wettbewerbsrecht Markenrecht, 11. Aufl. 2011</li> <li>- Rehbinder/Peukert, Urheberrecht, 18. Aufl. 2018</li> <li>- Schack, Urheber- und Urhebervertragsrecht, 8. Aufl. 2017</li> <li>- Sosnitza, Deutsches und europäisches Markenrecht, 2. Aufl. 2015</li> <li>- Bunte/Stancke, Kartellrecht, 3. Aufl. 2015</li> <li>- Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018</li> <li>- Kallwass/Abels, Privatrecht, 23. Aufl. 2018</li> <li>- Medicus/Petersen, Grundwissen zum Bürgerlichen Recht, 10. Aufl. 2014</li> </ul>

<b>LEHRVERANSTALTUNG: Urheber- und Computerrecht</b>	
<b>Art</b>	Vorlesung
<b>Nr.</b>	M+I150
<b>SWS</b>	2,00 SWS
<b>Lerninhalt</b>	<ul style="list-style-type: none"> <li>- Grundlagen der Medien-, Meinungs- und Informationsfreiheit, Recht aus informationelle Selbstbestimmung, Unrechtsbewusstsein, Strafbestände und Vorgehensweisen</li> <li>- Betrug und Computerbetrug, Urkundenfälschung im Computer, Strafbarkeit des Abfahgens und Ausspähen von Daten, Datenveränderung und Computersabotage, Schutzbereiche der Datenschutznormen</li> <li>- Internetstrafrecht: Verletzung von Urheberrechten, Extremistische Propaganda, Pornographie und Glücksspiel, strafrechtliche Behandlung von Internet-Providern</li> <li>- Befugnis zu IT-Sicherheitsprüfungen, Zulässigkeit von Hackertools</li> </ul>
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

## 4. Semester

UNITS-30: Sicherheit in Webapplikationen

UNITS-31: Netzwerk-Sicherheit

UNITS-32: Sicherheitsmanagement und Unternehmensprozesse

UNITS-33: Unternehmenspraxis

## UNITS-30: Sicherheit in Webapplikationen

<b>Empfohlene Vorkenntnisse</b>	Kenntnisse von Betriebssystemen und Netzwerken	
<b>Lehrform</b>	Vorlesung/Seminar/Labor	
<b>Lernziele</b>	<p>Wissen (1): Nach erfolgreicher Teilnahme am Modul können die Studierenden...</p> <ul style="list-style-type: none"> <li>typische Verwundbarkeiten von WebApplikationen sowie von Webservern verstehen und beschreiben</li> <li>charakteristische Sicherheitsprobleme erkennen, die bei der Erstellung von WebApplikationen zu berücksichtigen sind</li> </ul> <p>Verständnis (2): Nach erfolgreicher Teilnahme am Modul können die Studierenden...</p> <ul style="list-style-type: none"> <li>die OWASP Top-Ten Sicherheitsrisiken für Webapplikation verstehen und einordnen</li> <li>empfohlene Gegenmaßnahmen hinsichtlich der zu erbringenden Schutzziele verstehen und einordnen</li> </ul> <p>Anwendung (3): Nach erfolgreicher Teilnahme am Modul können die Studierenden...</p> <ul style="list-style-type: none"> <li>Sicherheitsprobleme benennen sowie Gegenmaßnahmen bei der Erstellung von WebApplikationen umsetzen können praxismgerechte Architekturentscheidungen basierend auf den vom BSI empfohlenen Best-Practices treffen</li> </ul> <p>Analyse (4): Nach erfolgreicher Teilnahme am Modul können die Studierenden...</p> <ul style="list-style-type: none"> <li>konkrete WebApplikationen anhand grundlegender Verwundbarkeiten analysieren und kritisch beurteilen</li> </ul>	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	6 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	150,00 h
	Workload:	240,00 h
<b>ECTS</b>	7,50 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	K60, LA, RE	
<b>Modulverantwortung</b>	Dirk Westhoff	
<b>Empfohlenes Semester</b>	4. Semester	
<b>Häufigkeit</b>	jedes Jahr (SS)	
<b>Verwendbarkeit</b>	BA UNITS und weitere Studiengänge	

<b>LEHRVERANSTALTUNG: Privacy</b>	
<b>Art</b>	Seminar
<b>Nr.</b>	M+I242
<b>SWS</b>	2,00 SWS
<b>Lerninhalt</b>	Bei dieser Seminarveranstaltung wird von den Teilnehmern erwartet, dass sie zu einem selbst gewählten Thema eine wissenschaftliche

	Ausarbeitung und an einem Präsenztermin dazu einen Vortrag mit anschließender Diskussion halten. Das vorgegebene Themenfeld umfasst sowohl Grundlagen als auch tagesaktuelle Fragestellungen zu Privacy und verwandten Themen. Die Spanne reicht hier von technisch ausgerichteten Themen bis hin zu gesellschaftlichen und ethischen Fragestellungen und Trends auf dem Gebiet der modernen technischen Entwicklung.
Lehrveranstaltungs- sprache	de
Literatur	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

<b>LEHRVERANSTALTUNG: Sicherheit in Webapplikationen</b>	
Art	Vorlesung
Nr.	M+I274
SWS	2,00 SWS
Lerninhalt	<ul style="list-style-type: none"> <li>- Allgemeine Maßnahmen der Informationssicherheit, 3-Schichten Architektur</li> <li>- OWASP Top-Ten Sicherheitsrisiken</li> <li>- Sicherheitsbetrachtung bei der Nutzung von mobilen Code (ActiveX, Java, JavaScript, PHP)</li> <li>- Absicherung von Webapplikationen gegen SQL-Injection, XSS, XSRF und andere</li> <li>- DoS, DDoS und Härten von WebServern</li> <li>- Transport Layer Security und PKI</li> <li>- DNS und DNSSEC</li> </ul>
Lehrveranstaltungs- sprache	de
Literatur	<ul style="list-style-type: none"> <li>- Simson Garfinkel, Gene Spafford, Web Security, Privacy &amp; Commerce, O'Reilly, 2nd Edition, ISBN-10: 0596000456</li> <li>- Stuart McClure, Joel Scambray, Georg Kurtz, Mc Graw Hill, Hacking Exposed 7, Network Security &amp; Solutions, 7th edition, O'Reilly, ISBN: 9780071780285</li> <li>- P. Gorski, L. Lo Iacono, H. Nguyen, Wbsockets - Moderne HTML5-Echtzeitanwendungen entwickeln, Carl Hanser, München, Wien 2015, ISBN 978-3-446-44371-6</li> <li>- Tim Phillip Schäfers, Hacking im Web, EAN: 9783645606363</li> </ul>

<b>LEHRVERANSTALTUNG: Labor Sicherheit in Webapplikationen</b>	
Art	Labor
Nr.	M+I280
SWS	2,00 SWS
Lerninhalt	
Lehrveranstaltungs- sprache	de
Literatur	

## UNITS-31: Netzwerk-Sicherheit

Empfohlene Vorkenntnisse	Netzwerkkenntnisse	
Lehrform	Vorlesung/Labor	
Lernziele	<p>Die Lernziele beim Erwerb von Fachwissen beinhalten</p> <ul style="list-style-type: none"> <li>- das Kennenlernen Kryptographischer, sowie ihre Verwendung in verschiedenen Netzwerkprotokollen bewerten können</li> <li>- das strukturierte Vorgehen bei der Planung und Umsetzung von Unternehmensnetzen sowie deren Umsetzung bewerten können</li> </ul> <p>Weitere Lernziele sind das Verständnis und die Analyse von</p> <ul style="list-style-type: none"> <li>- ausgewählten Sicherheitsprotokollen und Diensten drahtgebundener Netzwerke sowie das gebotene Sicherheitsniveau einordnen und analysieren können</li> <li>- ausgewählten Sicherheitsprotokollen und Diensten drahtloser Netzwerke sowie das gebotene Sicherheitsniveau analysieren können</li> </ul>	
Dauer	1 Semester	
SWS	6 SWS	
Aufwand	Lehrveranstaltung:	90,00 h
	Selbststudium/Gruppenarbeit:	120,00 h
	Workload:	210,00 h
ECTS	7,50 ECTS	
Voraussetzungen für die Vergabe von LP	Klausurarbeit, 90 Min.	
Modulverantwortung	Prof. Dr. Dirk Westhoff	
Empfohlenes Semester	4. Semester	
Häufigkeit	jedes Jahr (SS)	
Verwendbarkeit	BA UNITS	

<b>LEHRVERANSTALTUNG: Netzwerks-Sicherheitskomponenten</b>	
Art	Labor
Nr.	M+I237
SWS	2,00 SWS
Lerninhalt	
Lehrveranstaltungs-sprache	de
Literatur	Vorlesungsrelevante Literatur wird in der Veranstaltung/über Moodle bekannt gegeben.

<b>LEHRVERANSTALTUNG: Netzwerkplanung &amp; -management</b>	
Art	Vorlesung
Nr.	M+I244

SWS	2,00 SWS
Lerninhalt	
Lehrveranstaltungs-sprache	de
Literatur	- Patrick-Benjamin Bök, York Tüchelmann, Planung und Auslegung von Computernetzen, Systematik und metodische Vorgehensweise, W3L-Verlag - J. McCabe, Network Analysis, Architecture, and Design, 3rd edition, Morgan Kaufmann

<b>LEHRVERANSTALTUNG: Sichere Netze</b>	
Art	Vorlesung
Nr.	M+I295
SWS	2,00 SWS
Lerninhalt	Die folgenden Lerninhalte sind Gegenstand der Veranstaltung - Grundlagen der Kryptographie (Stromchiffren, Public-Key Kryptographie, Digitale Signaturen, Hashfunktionen, MAC, DH, ECDH) - Erörterung der Verwendung kryptografischer Bausteine in ausgewählten Sicherheitsprotokollen und Diensten drahtgebundener Netze, wie IPsec/IKE, TLS , DNSSEC, Paketfiler und Applikation Gateways - Erörterung der Verwendung kryptografischer Bausteine in ausgewählten Sicherheitsprotokollen und Diensten drahtloser Netze, wie Sicherheit für Mobilfunknetze, Sicherheit für drahtlose lokale Netze
Lehrveranstaltungs-sprache	de
Literatur	- Claudia Eckert, IT-Sicherheit, Konzepte Verfahren Protokolls, 5te Auflage, Oldenbour Verlag - Christof Paar, Jan Pelzl, Understanding Cryptography, A Textbook for Students and Practioners, Springer - S. McClure, J. Scambray, G. Kurtz, Hacking Exposed 7, Network Security & Solutions

## UNITS-32: Sicherheitsmanagement und Unternehmensprozesse

Empfohlene Vorkenntnisse	Organisatorische Grundkenntnisse sowie Grundlagen der BWL.
Lehrform	Vorlesung/Seminar
Lernziele	Die Studierenden können nach Beendigung des Moduls - ...Fakten, Wissen und Konzepte erlernen bezüglich des Prozessmanagements, Prozessanalyse und Prozessimplementierung sowie der Personal-, Unternehmensführung sowie dem Umgang mit Geschäftspartnern, - ...Kernideen der Vorlesungen verstehen, für sich organisieren, interpretieren und selbständig beschreiben bezüglich des Prozessmanagements, Prozessanalyse und Prozessimplementierung sowie der Personal-, Unternehmensführung sowie dem Umgang mit

	Geschäftspartnern, - ...das erworbene Wissen in neuen Situationen für eine Problemlösung heranziehen bezüglich des Prozessmanagements, Prozessanalyse und Prozessimplementierung sowie der Personal-, Unternehmensführung sowie dem Umgang mit Geschäftspartnern, - ...komplexere Sachverhalte aufbrechen, um neues anwendungsbezogenes Wissen zu generieren bezüglich des Prozessmanagements, Prozessanalyse und Prozessimplementierung sowie der Personal-, Unternehmensführung sowie dem Umgang mit Geschäftspartnern.	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	4 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
<b>ECTS</b>	5,00 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	Modulprüfung/Mündliche Prüfung (20 Minuten) - UNITS208 Prozess-Management (2,5 Credits) - UNITS209 Personalführung & Umgang mit Geschäftspartnern (2,5 Credits)	
<b>Modulverantwortung</b>	Prof. Dr. rer. soc. HSG Dirk Drechsler	
<b>Empfohlenes Semester</b>	4. Semester	
<b>Häufigkeit</b>	jedes Jahr (SS)	
<b>Verwendbarkeit</b>	Bachelor UNITS Bachelor MI	

<b>LEHRVERANSTALTUNG: Prozess-Management</b>	
<b>Art</b>	Vorlesung
<b>Nr.</b>	M+I238
<b>SWS</b>	2,00 SWS
<b>Lerninhalt</b>	- Grundlagen - Entwicklung von Geschäftsprozessen - Systeme und Dokumentation - Prozesse und Kontrollen - Order-to-Cash - E-Business - Data Analytics
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	- Beynon-Davies, Paul; Business Information Systems; Palgrave; aktuelle Auflage. - Beynon-Davies, Paul; eBusiness; Palgrave; aktuelle Auflage. - Gelinas, Ulric J. et al.; Accounting Information Systems; Cengage; aktuelle Auflage. - Freund, Jakob; Rücker, Bernd; Praxishandbuch BPMN 2.0; Hanser; aktuelle Auflage. - Hall, James A.; Accounting Information Systems; Cengage; aktuelle

	Auflage. - Hurt, Robert L.; Accounting Information Systems; McGrawHill; aktuelle Auflage. - Kavanagh, Michael J. et al.; Human Resources Information Systems; Sage; aktuelle Auflage. - Richardson, Vernon J. et al.; Accounting Information Systems; McGrawHill; aktuelle Auflage.
--	--

<b>LEHRVERANSTALTUNG: Personalführung &amp; Umgang mit Geschäftspartnern</b>	
Art	Seminar
Nr.	M+I239
SWS	2,00 SWS
Lerninhalt	
Lehrveranstaltungs- sprache	de
Literatur	

## UNITS-33: Unternehmenspraxis

Empfohlene Vorkenntnisse	Kenntnisse einer Programmiersprache, Datenbanken	
Lehrform	Vorlesung/Labor	
Lernziele	- Die Studierenden kennen und verstehen die wichtigen E-Business Software Systeme, deren Architektur und Funktionsweise vor allem in Hinblick auf Sicherheitsaspekte - Sie können E-Business Applikationen unter Beachtung von Sicherheitsrestriktionen bedienen, konfigurieren und anpassen	
Dauer	1 Semester	
SWS	2 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
ECTS	30,00 ECTS	
Voraussetzungen für die Vergabe von LP	Klausurarbeit, 90 Min. und Praktische Arbeit (E-Business-Applikationen, Praktikum E-Business-Applikationen)	
Modulverantwortung	Prof. Dr. Volker Sänger	
Empfohlenes Semester	4. Semester	
Häufigkeit	jedes Jahr (SS)	
Verwendbarkeit	BA UNITS	

<b>LEHRVERANSTALTUNG: Praxisarbeit</b>	
Art	Seminar
Nr.	M+I188

SWS	2,00 SWS
Lerninhalt	Unternehmens- und IT-Sicherheit
Lehrveranstaltungs- sprache	de
Literatur	freie Wahl

<b>LEHRVERANSTALTUNG: Praktisches Studiensemester</b>	
Art	Praktikum
Nr.	M+I302
SWS	0,00 SWS
Lerninhalt	Das Ableisten des Praktischen Studiensemesters erfolgt in medienspezifischen Unternehmen. Ziel des Praktischen Studiensemesters ist die Anwendung des erworbenen Wissens und der erworbenen Fähigkeiten und Fertigkeiten der vorangegangenen Studiensemester. Die Studierenden sollen hierbei anhand konkreter Aufgabenstellungen einen tiefer gehenden Einblick in das vielschichtige Berufsfeld der Medienwirtschaft erhalten. Ziel ist die Vermittlung von gestalterischen, organisatorischen, wirtschaftlichen und technischen Zusammenhängen. 95 Präsenztage (35 Stunden pro Woche = mindestens 665 Stunden)
Lehrveranstaltungs- sprache	de
Literatur	

# 5. Semester

## UNITS-35: Projektarbeit

## UNITS-35: Projektarbeit

<b>Empfohlene Vorkenntnisse</b>	Inhalt der Module UNITS-14 Sicherheit & Unternehmenskultur (Strategie, Organisation, Corporate Governance, Compliance, Sicherheitsstandards, mathematische Statistik) UNITS-32 Sicherheitsmanagement und Unternehmensprozesse (Prozessmanagement, Informationssysteme)
<b>Lehrform</b>	Vorlesung
<b>Lernziele</b>	Die Studierenden können nach Beendigung des Moduls - ...Fakten, Wissen und Konzepte erlernen bezüglich der Risk Intelligence, des Risikomanagements, des Business Continuity und Disaster Recovery Managements sowie der quantitativen Risikoanalyse, - ...Kernideen der Vorlesungen verstehen, für sich organisieren, interpretieren und selbständig beschreiben bezüglich der Risk Intelligence, des Risikomanagements, des Business Continuity und Disaster Recovery Managements sowie der quantitativen Risikoanalyse, - ...das erworbene Wissen in neuen Situationen für eine Problemlösung heranziehen bezüglich der Risk Intelligence, des Risikomanagements, des Business Continuity und Disaster Recovery Managements sowie der quantitativen Risikoanalyse, - ...komplexere Sachverhalte aufbrechen, um neues anwendungsbezogenes Wissen zu generieren bezüglich der Risk Intelligence, des Risikomanagements, des Business Continuity und Disaster Recovery Managements sowie der quantitativen Risikoanalyse.
<b>Dauer</b>	1 Semester
<b>SWS</b>	4 SWS
<b>Aufwand</b>	Lehrveranstaltung: 90,00 h
	Selbststudium/Gruppenarbeit: 120,00 h
	Workload: 210,00 h
<b>ECTS</b>	10,00 ECTS
<b>Voraussetzungen für die Vergabe von LP</b>	Modulprüfung (K90 - 90 Minuten) - UNITS216 Risikomanagement (5 Credits) - UNITS218 Business Continuity & Disaster Recovery (2 Credits)
<b>Modulverantwortung</b>	Prof. Dr. rer. soc. HSG Dirk Drechsler
<b>Empfohlenes Semester</b>	5. Semester
<b>Häufigkeit</b>	jedes Jahr (SS)
<b>Verwendbarkeit</b>	BA UNITS BA MI

<b>LEHRVERANSTALTUNG: Projektarbeit</b>	
<b>Art</b>	Seminar
<b>Nr.</b>	M+I303
<b>SWS</b>	4,00 SWS
<b>Lerninhalt</b>	Bearbeitung eines vorgegebenen Themas im Team (typ. 4 bis 5 Studierende) nach den Regeln des Projektmanagements

Lehrveranstaltungs- sprache	de
Literatur	Wird bei Bedarf vom Betreuer bekanntgegeben.

# 6. Semester

UNITS-34: Sicherheits- und Risikomanagement

UNITS-36: Computer-Forensik

## UNITS-34: Sicherheits- und Risikomanagement

Empfohlene Vorkenntnisse	
Lehrform	Seminar/Vorlesung/Praxis
Lernziele	<p>Lernziele</p> <ul style="list-style-type: none"> <li>- Anwenden des im Studium Gelernten im Unternehmen: was bedeutet IT-Sicherheit für ein Unternehmen?</li> <li>- Managen von Projekten</li> <li>- Kennen, verstehen, und umsetzen von Privacy-Konzepten und rechtlicher Aspekte des Datenschutzes/der Datensicherheit im Unternehmen</li> </ul> <p>Inhalt</p> <ul style="list-style-type: none"> <li>- Datenschutz, Sicherheit und deren rechtliche Aspekte</li> <li>- Management von IT-Sicherheitsprojekten</li> <li>- IT-Sicherheitspraxis</li> </ul>
Dauer	1 Semester
SWS	6 SWS
Aufwand	Lehrveranstaltung: 90,00 h
	Selbststudium/Gruppenarbeit: 750,00 h
	Workload: 840,00 h
ECTS	7,50 ECTS
Voraussetzungen für die Vergabe von LP	Referat + Hausarbeit + Referat + BE/KO
Modulverantwortung	Prof. Dr. Daniel Hammer
Empfohlenes Semester	6. Semester
Häufigkeit	jedes Jahr (SS)
Verwendbarkeit	BA UNITS

<b>LEHRVERANSTALTUNG: Risikomanagement</b>	
Art	Vorlesung
Nr.	M+I246
SWS	4,00 SWS
Lerninhalt	<ul style="list-style-type: none"> <li>- Marktorientierte Risikoperspektive zum Einstieg</li> <li>- Sind Risikomanager zu negativ?</li> <li>- Globale Risiken und Unternehmenssicherheit</li> <li>- Unternehmerische Komplexität</li> <li>- Integrative Methodik</li> <li>- Die dreistufige Analyse</li> <li>- Früherkennung und Funktionen</li> <li>- Risikomanagement nach anerkannten Methoden</li> </ul>
Lehrveranstaltungs-sprache	de
Literatur	<ul style="list-style-type: none"> <li>- COSO (Ed.); Enterprise Risk Management - Integrated Framework; COSO; aktuelle Auflage.</li> <li>- Project Management Institute (Ed.); Navigating Complexity; PMI; 2014.</li> </ul>

	- Talabis, Mark Ryan M.; Martin, Jason L.; Information Security Risk Assessment Toolkit; Syngres; 2013.
--	---

<b>LEHRVERANSTALTUNG: Business Continuity &amp; Disaster Recovery</b>	
Art	Vorlesung
Nr.	M+I248
SWS	2,00 SWS
Lerninhalt	1. Root Cause Analysis 2. Business Continuity Management
Lehrveranstaltungs- sprache	de
Literatur	- Heuvel, Lee N. Vanden et al. (Hrsg.); Root Cause Analysis Handbook; Third Ed.; Rothstein; 2008. - Hiles, Andrew; Business Continuity Management; Fourth Ed.; Rothstein; 2014. - Engemann, Kurt J. et al.; Business Continuity and Risk Management; Rothstein; 2012. - Graham, Julia et al.; A Risk Management Approach to Business Continuity; Rothstein; 2006.

## UNITS-36: Computer-Forensik

Empfohlene Vorkenntnisse	
Lehrform	Seminar
Lernziele	<p>Lernziele</p> <ul style="list-style-type: none"> <li>- Darstellung gelernter Inhalte über die Wiedergabe von Fakten, grundlegenden Konzepten und Antworten mit Bezug auf die Fächer Praktische Unternehmens- &amp; IT-Sicherheit.</li> <li>- Demonstration des Verständnisses bezüglich Fakten und Ideen mittels Organisation, Übersetzung, Interpretation, Beschreibung und Vertreten von Kernideen mit Bezug auf die Fächer Praktische Unternehmens- &amp; IT-Sicherheit.</li> <li>- Verwendung des erworbenen Wissens. Problemlösung in neuen Situationen über die Anwendung erworbenen Wissens, Fakten, Techniken und Regeln mit Bezug auf die Fächer Praktische Unternehmens- &amp; IT-Sicherheit.</li> <li>- Untersuchung und Aufbrechen von Informationen in ihre Bestandteile mittels der Identifikation von Motiven und Gründen. Bildung von Rückschlüssen und Auffinden von Beweisen, um Verallgemeinerungen zu stützen mit Bezug auf die Fächer Praktische Unternehmens- &amp; IT-Sicherheit.</li> <li>- Aufbau von Strukturen und Muster auf der Grundlage diverser Elemente; dies umfasst auch die Zusammenführung von Bestandteilen, um neue Muster oder alternative Lösungen zu entwickeln mit Bezug auf die Fächer Praktische Unternehmens- &amp; IT-Sicherheit.</li> <li>- Präsentation und Verteidigung von Meinungen durch die Beurteilung</li> </ul>

	von Informationen, Gültigkeit von Ideen oder Qualität der Arbeit auf der Grundlage vordefinierter Kriterien mit Bezug auf die Fächer Praktische Unternehmens- & IT-Sicherheit.	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	6 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	30,00 h
	Selbststudium/Gruppenarbeit:	120,00 h
	Workload:	150,00 h
<b>ECTS</b>	7,50 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	Praktikum/Praxisarbeit - UNITS219 Praxisarbeit (5 Credits)	
<b>Modulverantwortung</b>	Prof. Dr. rer. soc. HSG Dirk Drechsler	
<b>Empfohlenes Semester</b>	6. Semester	
<b>Häufigkeit</b>	jedes Jahr (SS)	
<b>Verwendbarkeit</b>	BA UNITS	

<b>LEHRVERANSTALTUNG: Computer als Tatwerkzeug</b>	
<b>Art</b>	Seminar
<b>Nr.</b>	M+I251
<b>SWS</b>	2,00 SWS
<b>Lerninhalt</b>	<ul style="list-style-type: none"> <li>- Cyberkriminellen auf der Spur, Besonderheiten multimedialer Kriminalität, von Tätern und deren Motivationen (nicht nur) im Unternehmensumfeld</li> <li>- Ziele der Computer-Forensik, ihre grundlegenden Fragestellungen und Methoden</li> <li>- Das Locardsche Austauschprinzip und digitale Beweismittel</li> <li>- Grundlagen maschinennaher Informationsdarstellung, Systeminformationen und Interna unterschiedlicher Betriebssysteme aus forensischer Sicht</li> <li>- Tatortsicherung: elektronische Beweissicherung und der forensische Prozess, Erstellen bitgetreuer Datenträger-Kopien, Post-mortem-analyse und Live-Untersuchung</li> <li>- Rechtliches Umfeld von Cyberkriminalität und forensischen Ermittlungen</li> </ul>
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	Begleitmaterial, Literaturempfehlungen und Toolsammlungen werden den Teilnehmern zum Vorlesungsstart zur Verfügung gestellt

<b>LEHRVERANSTALTUNG: Computer Forensik</b>	
<b>Art</b>	Vorlesung
<b>Nr.</b>	M+I252
<b>SWS</b>	3,00 SWS
<b>Lerninhalt</b>	- Bitgetreue Datensicherung in Theorie und Praxis, Forensische

	Duplikation, Schichten der Datenerfassung, Datenstrukturen, Strings und Character Encodings, Physikalische Adressen - Hardwarespezifikationen, Host Protected Area, Device Configuration Overlay, Verschlüsselung von Datenträgern, NTFS Alternate Data Streams, File Slack, etc. - Datenanalyse und -manipulation: Finden + Verstecken + Vernichten von Daten, Forensische Analyse mobiler Datenträger, Analyse von digitalem Bildmaterial - Forensische Analyse-Werkzeuge in Theorie und Praxis
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	Begleitmaterial, Literaturempfehlungen und Toolsammlungen werden den Teilnehmern zum Vorlesungsstart zur Verfügung gestellt.

<b>LEHRVERANSTALTUNG: Labor Computer Forensik</b>	
<b>Art</b>	Labor
<b>Nr.</b>	M+I253
<b>SWS</b>	1,00 SWS
<b>Lerninhalt</b>	- Erstellung forensischer Images und deren Post-mortem-Analyse - Live-Forensik mit Hauptspeicheranalyse an kompromittierten Systemen - NTFS Alternate Data Streams
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	

## 7. Semester

UNITS-66: Security Analysen & Pentesting

UNITS-37: International Security Trends

UNITS-38: Bachelorarbeit

UNITS-61: Reverse Engineering

UNITS-62: Penetration Testing

UNITS-63: Verlässliche verteilte Systeme

UNITS-64: Prävention & Krisenmanagement

UNITS-65: Red Teaming & IT Infrastruktur Sicherheit

UNITS-67: Applied Cryptanalysis

## UINITS-66: Security Analysen & Pentesting

Empfohlene Vorkenntnisse	
Lehrform	Vorlesung/Labor
Lernziele	
Dauer	1 Semester
SWS	4 SWS
Aufwand	Lehrveranstaltung: 60,00 h
	Selbststudium/Gruppenarbeit: 90,00 h
	Workload: 150,00 h
ECTS	5,00 ECTS
Voraussetzungen für die Vergabe von LP	
Modulverantwortung	
Empfohlenes Semester	7. Semester
Häufigkeit	jedes Jahr (WS)
Verwendbarkeit	

LEHRVERANSTALTUNG: Security Analysen & Pentesting	
Art	Vorlesung
Nr.	M1202
SWS	2,00 SWS
Lerninhalt	
Lehrveranstaltungs-sprache	de
Literatur	

LEHRVERANSTALTUNG: Labor Security Analyse & Pentesting	
Art	Labor
Nr.	M1203
SWS	2,00 SWS
Lerninhalt	
Lehrveranstaltungs-sprache	de
Literatur	

## UNITS-37: International Security Trends

Empfohlene Vorkenntnisse	Modul Unternehmenspraxis, insb. Veranstaltung Projektmanagement
Lehrform	Seminar

<b>Lernziele</b>	Die Studierenden lernen, das bisher im Studium theoretisch und praktisch erworbene Wissen in einem anspruchsvollen Projekt unter professionellen Bedingungen praxisgerecht und im Team umzusetzen. Sie vertiefen hierbei Ihr Fachwissen und Ihre Methodenkompetenz.	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	4 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	180,00 h
	Workload:	240,00 h
<b>ECTS</b>	5,00 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	Projektarbeit	
<b>Modulverantwortung</b>	Prof. Dr. Dirk Westhoff	
<b>Empfohlenes Semester</b>	7. Semester	
<b>Häufigkeit</b>	jedes Semester	
<b>Verwendbarkeit</b>	UNITS	

<b>LEHRVERANSTALTUNG: Security Trends</b>	
<b>Art</b>	Seminar
<b>Nr.</b>	M+I254
<b>SWS</b>	2,00 SWS
<b>Lerninhalt</b>	Die Lerninhalte dieser Veranstaltung ist die kritische fachliche Auseinandersetzung mit aktuellen Trends der technischen sowie der organisatorischen Sicherheit. Im Rahmen einer schriftlichen Ausarbeitung werden aktuelle Themen der IT-Sicherheit analysiert und in Bezug zu dem, in den vorherigen UNITS Veranstaltungen erworbenen Wissen gesetzt. Ein wesentliches Lernziel ist es dabei das erworbene Wissen in neuen Situationen für eine Problemlösung zu verwenden und einzuordnen. Im Idealfall kann dann hieraus weiteres, anwendungsbezogenes Wissen geschöpft werden welches passgenau zur Tagesaktualität einer sich ständig ändernden Bedrohungslage ist.
<b>Lehrveranstaltungs-sprache</b>	de
<b>Literatur</b>	Das Wesen der Veranstaltung ist die kritische Auseinandersetzung mit aktuellen Themen ist für die oftmals keine 'Standardliteratur' vorhanden ist. Daher ist die Suche nach verwendbarer Literatur ein Aspekt bei der Auseinandersetzung mit dem zu erarbeitenden Thema.

<b>LEHRVERANSTALTUNG: Datenschutz, Unternehmens- &amp; IT-Sicherheit im internationalen Umfeld</b>	
<b>Art</b>	Seminar
<b>Nr.</b>	M+I255
<b>SWS</b>	2,00 SWS
<b>Lerninhalt</b>	Es werden je nach Aktualität folgende Themen erarbeitet und Inhalte vermittelt:

	<ul style="list-style-type: none"> <li>- Fallstudienanalysen zur Informationssicherheit und IT-Risikomanagement.</li> <li>- DSGVO (Datenschutzgrundverordnung)</li> <li>- LINDUNN (Privacy Impact Assessment)</li> <li>- STRIDE (Threat Modelling)</li> </ul>
<b>Lehrveranstaltungs- sprache</b>	de
<b>Literatur</b>	Härtling, Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis Gebundenes Buch - 17. Juni 2016 Verlag Dr. Otto Schmidt; Auflage: 1. Shostack Threat Modeling: Designing for Security (Englisch) Taschenbuch - Wiley; Auflage: 1. (7. Februar 2014) Ausgewählte aktuelle Papiere und Studien zu organisatorischen und technischen Datenschutz (GI, ACM, IEEE).

## UNITS-38: Bachelorarbeit

<b>Empfohlene Vorkenntnisse</b>	Kenntnisse der IT-Sicherheit und Betriebssysteme	
<b>Lehrform</b>	Vorlesung/Seminar/Labor	
<b>Lernziele</b>	Einführung in grundlegende Verfahren, technische Hintergründe und Details bei der Untersuchung von Spuren krimineller Aktionen im Zusammenhang mit IT-Systemen	
<b>Dauer</b>	1 Semester	
<b>SWS</b>	2 SWS	
<b>Aufwand</b>	Lehrveranstaltung:	90,00 h
	Selbststudium/Gruppenarbeit:	120,00 h
	Workload:	210,00 h
<b>ECTS</b>	15,00 ECTS	
<b>Voraussetzungen für die Vergabe von LP</b>	K60, RE, LA	
<b>Modulverantwortung</b>	Prof. Dr. rer. nat. Daniel Hammer	
<b>Empfohlenes Semester</b>	7. Semester	
<b>Häufigkeit</b>	jedes Jahr (SS)	
<b>Verwendbarkeit</b>	BA UNITS	

<b>LEHRVERANSTALTUNG: Bachelor Thesis</b>	
<b>Art</b>	Wissenschaftl. Arbeit/Seminar
<b>Nr.</b>	M+I308
<b>SWS</b>	0,00 SWS
<b>Lerninhalt</b>	
<b>Lehrveranstaltungs- sprache</b>	de
<b>Literatur</b>	

<b>LEHRVERANSTALTUNG: Präsentation &amp; Verteidigung</b>	
Art	Seminar
Nr.	M+I309
SWS	2,00 SWS
Lerninhalt	
Lehrveranstaltungs- sprache	de
Literatur	

## UNITS-61: Reverse Engineering

Empfohlene Vorkenntnisse	Kenntnisse des Grundstudiums zu Betriebssystemen sowie IT-Sicherheit und Programmierung.	
Lehrform	Vorlesung/Labor	
Lernziele	Dem / der Studierenden sollen einfache Grundkonzepte und Techniken des Reverse Engineerings sowie relevante Sicherheitsaspekte vermittelt werden: - Aufbau des Speichers - Register - Analyse von Programmcode (Binary) - Einsatz von Debugger und Analysetools (IDAPro)	
Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP	Klausurarbeit, 60 Min. und Laborarbeit (Reverse Engineering, Labor Reverse Engineering)	
Modulverantwortung	Prof. Dr. Andreas Schaad	
Empfohlenes Semester	7. Semester	
Häufigkeit	jedes Jahr (WS)	
Verwendbarkeit	BA UNITS	

## UNITS-62: Penetration Testing

Empfohlene Vorkenntnisse	Kenntnisse aus dem Bereich IT-Sicherheit und Netzwerktechnologie	
Lehrform	Vorlesung/Labor	
Lernziele	Die / der Studierende soll: - Vorgehensweisen und Techniken zur Analyse moderner IT-Infrastrukturen, Betriebssysteme und Applikationsumgebungen kennen und anwenden lernen	

	- Einsatz komplexer Methoden, Tools und Techniken für professionelle Analysen und Beratungen in der IT-Sicherheit verstehen und durchführen können - Den Aufbau von komplexen IT Systemen analysieren können Sie / er kann danach erste industrielle PenTests durchführen.
<b>Dauer</b>	1 Semester
<b>SWS</b>	4 SWS
<b>Aufwand</b>	Lehrveranstaltung: 60,00 h
	Selbststudium/Gruppenarbeit: 90,00 h
	Workload: 150,00 h
<b>ECTS</b>	5,00 ECTS
<b>Voraussetzungen für die Vergabe von LP</b>	Klausurarbeit, 60 Min. und Laborarbeit (Penetration Testing, Labor Penetration Testing)
<b>Modulverantwortung</b>	Prof. Dr. Andreas Schaad
<b>Empfohlenes Semester</b>	7. Semester
<b>Häufigkeit</b>	jedes Jahr (WS)
<b>Verwendbarkeit</b>	BA UNITS

## UNITS-63: Verlässliche verteilte Systeme

<b>Empfohlene Vorkenntnisse</b>	Computernetze, Betriebssysteme
<b>Lehrform</b>	Vorlesung/Labor
<b>Lernziele</b>	<p>Wissen (1): Nach erfolgreicher Teilnahme am Modul können die Studierenden Charakteristische Eigenschaften, sowie Vor- &amp; Nachteile von verteilten Systemen im Vergleich zu zentralen Systemen beschreiben, typische Designprobleme erkennen, die sich beim Übergang von zentralen zu verteilten Systemen ergeben</p> <p>Verständnis (2): Nach erfolgreicher Teilnahme am Modul können die Studierenden... die klassischen Zielkonflikte bzgl. Entwurfsformen verteilter Systeme verstehen und einordnen die Bedeutung von mehrseitiger Sicherheit für heterogene verteilte Umgebungen verstehen und einordnen</p> <p>Anwendung (3): Nach erfolgreicher Teilnahme am Modul können die Studierenden... praxisgerechte Architekturentscheidungen hinsichtlich Sicherheit, Verfügbarkeit &amp; Fehlertoleranz für verteilte Systeme treffen Sicherheitsprobleme sowie Sicherheitserweiterungen in verteilten Systemen benennen</p> <p>Analyse (4): Nach erfolgreicher Teilnahme am Modul können die Studierenden... Verteilte Systeme anhand grundlegender Charakteristika analysieren und kritisch beurteilen Betrachtungen zu Skalierbarkeit, Transparenz, Verfügbarkeit, Zuverlässigkeit und Sicherheit in verteilten heterogenen Systemen</p>

	analysieren und kritisch beurteilen Grundlegende Kommunikationsmodelle, Kommunikation mittels RPC/RMI, Multicast, Nachrichtenorientiert, Streamorientiert Verfahren/Protokolle zur Synchronisation, Konsistenz & Replikation Verfahren/Protokolle zur Sicherheit & Fehlertoleranz Rechteausweitung, Aspekte mehrseitiger Sicherheit, Privacy Enhancing Technologies analysieren und kritisch beurteilen	
Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP	K60 + LA	
Modulverantwortung	Prof. Dr. Dirk Westhoff	
Empfohlenes Semester	7. Semester	
Häufigkeit	jedes Jahr (WS)	
Verwendbarkeit	BA UNITS	

## UNITS-64: Prävention & Krisenmanagement

Empfohlene Vorkenntnisse	Grundlagen der IT Sicherheit	
Lehrform	Vorlesung	
Lernziele	Lernziele für die Studierenden sind: - Krisenvorsorgemaßnahmen planen und durchführen können - Krisenmanagement organisatorisch betreuen können - Adäquate Management- und Kommunikationsmaßnahmen im Krisenfall ergreifen können - Kritische Bereiche im Know-how und Arbeitsprozess eines Unternehmens erkennen können - Vorbeugende Maßnahmen gegenüber Manipulation und Wirtschaftsspionage ergreifen können	
Dauer	1 Semester	
SWS	4 SWS	
Aufwand	Lehrveranstaltung:	60,00 h
	Selbststudium/Gruppenarbeit:	90,00 h
	Workload:	150,00 h
ECTS	5,00 ECTS	
Voraussetzungen für die Vergabe von LP	K90	
Modulverantwortung	Prof. Dr. Andreas Schaad	
Empfohlenes Semester	7. Semester	
Häufigkeit	jedes Jahr (WS)	

Verwendbarkeit	BA UNITS
----------------	----------

## UNITS-65: Red Teaming & IT Infrastruktur Sicherheit

Empfohlene Vorkenntnisse	
Lehrform	Vorlesung/Labor
Lernziele	
Dauer	1 Semester
SWS	4 SWS
Aufwand	Lehrveranstaltung: 60,00 h
	Selbststudium/Gruppenarbeit: 90,00 h
	Workload: 150,00 h
ECTS	5,00 ECTS
Voraussetzungen für die Vergabe von LP	
Modulverantwortung	
Empfohlenes Semester	7. Semester
Häufigkeit	jedes Jahr (WS)
Verwendbarkeit	

## UNITS-67: Applied Cryptanalysis

Empfohlene Vorkenntnisse	
Lehrform	Vorlesung/Labor
Lernziele	
Dauer	1 Semester
SWS	4 SWS
Aufwand	Lehrveranstaltung: 60,00 h
	Selbststudium/Gruppenarbeit: 90,00 h
	Workload: 150,00 h
ECTS	5,00 ECTS
Voraussetzungen für die Vergabe von LP	
Modulverantwortung	
Empfohlenes Semester	7. Semester
Häufigkeit	jedes Jahr (WS)
Verwendbarkeit	

<b>LEHRVERANSTALTUNG: Applied Cryptanalysis</b>	
Art	Labor

Nr.	M379
SWS	4,00 SWS
Lerninhalt	
Lehrveranstaltungs- sprache	de
Literatur	