

# MODULHANDBUCH

**Bachelor of Science**

Bachelor Cyber Security (FS-BACSD)

**180 ECTS**

**Fernstudium**

Klassifizierung: Grundständig

# Inhaltsverzeichnis

---

## 1. Semester

### **Modul DLBIBRVS: Betriebssysteme, Rechnernetze und verteilte Systeme**

Modulbeschreibung .....	13
Kurs DLBIBRVS01: Betriebssysteme, Rechnernetze und verteilte Systeme .....	15

### **Modul DLBINGEDS: Einführung in Datenschutz und IT-Sicherheit**

Modulbeschreibung .....	21
Kurs DLBISIC01: Einführung in Datenschutz und IT-Sicherheit .....	23

### **Modul DLBBIMD: Mathematik: Analysis**

Modulbeschreibung .....	29
Kurs DLBBIMD01: Mathematik: Analysis .....	31

### **Modul DLBWIRITT: Einführung in das wissenschaftliche Arbeiten für IT und Technik**

Modulbeschreibung .....	35
Kurs DLBWIRITT01: Einführung in das wissenschaftliche Arbeiten für IT und Technik .....	37

### **Modul DLBDSIPWP\_D: Einführung in die Programmierung mit Python**

Modulbeschreibung .....	43
Kurs DLBDSIPWP01_D: Einführung in die Programmierung mit Python .....	45

### **Modul DLBDSSPDS\_D: Statistik - Wahrscheinlichkeit und deskriptive Statistik**

Modulbeschreibung .....	49
Kurs DLBDSSPDS01_D: Statistik - Wahrscheinlichkeit und deskriptive Statistik .....	51

---

## 2. Semester

### **Modul DLBINGOPJ: Grundlagen der objektorientierten Programmierung mit Java**

Modulbeschreibung .....	59
Kurs IOBP01: Grundlagen der objektorientierten Programmierung mit Java .....	61

### **Modul DLBBIM: Mathematik: Lineare Algebra**

Modulbeschreibung .....	67
Kurs DLBBIM01: Mathematik: Lineare Algebra .....	69

### **Modul DLBKA: Kollaboratives Arbeiten**

Modulbeschreibung .....	73
Kurs DLBKA01: Kollaboratives Arbeiten .....	75

**Modul DLBCSEINF\_D: Einführung in die Netzwerkforensik**

Modulbeschreibung .....	81
Kurs DLBCSEINF01_D: Einführung in die Netzwerkforensik .....	83

**Modul IREN: Requirements Engineering**

Modulbeschreibung .....	89
Kurs IREN01: Requirements Engineering .....	91

**Modul DLBCSESPB\_D: Grundzüge des System-Pentestings**

Modulbeschreibung .....	97
Kurs DLBCSESPB01_D: Grundzüge des System-Pentestings .....	99

---

**3. Semester****Modul DLBIHK: Interkulturelle und ethische Handlungskompetenzen**

Modulbeschreibung .....	107
Kurs DLBIHK01: Interkulturelle und ethische Handlungskompetenzen .....	109

**Modul DLBINGEIT: Einführung in das Internet of Things**

Modulbeschreibung .....	115
Kurs DLBINGEIT01: Einführung in das Internet of Things .....	117

**Modul DLBIADPS: Algorithmen, Datenstrukturen und Programmiersprachen**

Modulbeschreibung .....	123
Kurs DLBIADPS01: Algorithmen, Datenstrukturen und Programmiersprachen .....	125

**Modul DLBITIML: Theoretische Informatik und Mathematische Logik**

Modulbeschreibung .....	131
Kurs DLBITIML01: Theoretische Informatik und Mathematische Logik .....	133

**Modul IPMG-01: IT-Projektmanagement**

Modulbeschreibung .....	139
Kurs IPMG01-01: IT-Projektmanagement .....	141

**Modul DLBCSEDCSW\_D: DevSecOps und gängige Software-Schwachstellen**

Modulbeschreibung .....	147
Kurs DLBCSEDCSW01_D: DevSecOps und gängige Software-Schwachstellen .....	149

---

**4. Semester****Modul IWSM1: IT-Servicemanagement**

Modulbeschreibung .....	157
Kurs IWSM01: IT-Servicemanagement .....	159

<b>Modul DLBISIC2-01: Kryptografische Verfahren</b>	
Modulbeschreibung .....	165
Kurs DLBISIC02-01: Kryptografische Verfahren .....	167
<b>Modul DLBIITR: IT-Recht</b>	
Modulbeschreibung .....	173
Kurs DLBIITR01: IT-Recht .....	175
<b>Modul DLBCSEHSF_D: Host- und Softwareforensik</b>	
Modulbeschreibung .....	183
Kurs DLBCSEHSF01_D: Host- und Softwareforensik .....	185
<b>Modul DLBDSEAIS1_D: Artificial Intelligence</b>	
Modulbeschreibung .....	189
Kurs DLBDSEAIS01_D: Artificial Intelligence .....	191
<b>Modul DLBCSEISS_D: Standards der Informationssicherheit</b>	
Modulbeschreibung .....	195
Kurs DLBCSEISS01_D: Standards der Informationssicherheit .....	197
<hr/>	
<b>5. Semester</b>	
<b>Modul DLBCSSCTCS_D: Seminar: Aktuelle Themen in Computer Science</b>	
Modulbeschreibung .....	205
Kurs DLBCSSCTCS01_D: Seminar: Aktuelle Themen in Computer Science .....	207
<b>Modul DLBDSEDA1_D: Advanced Data Analysis</b>	
Modulbeschreibung .....	211
Kurs DLBDSEDA01_D: Advanced Data Analysis .....	213
<b>Modul DLBDSEDA2_D: Projekt: Data Analysis</b>	
Modulbeschreibung .....	217
Kurs DLBDSEDA02_D: Projekt: Data Analysis .....	219
<b>Modul DLBDSCC_D: Cloud Computing</b>	
Modulbeschreibung .....	223
Kurs DLBDSCC01_D: Cloud Computing .....	225
<b>Modul DLBCSEEISC_D: IT-Sicherheitsberatung</b>	
Modulbeschreibung .....	229
Kurs DLBCSEEISC01_D: Technische und betriebliche IT-Sicherheitskonzeptionen .....	232
Kurs DLBCSEEISC02_D: Projekt: Einsatz und Konfiguration von SIEM-Systemen .....	236
<b>Modul DLBCSEESE_D: Social Engineering</b>	

Modulbeschreibung .....	239
Kurs DLBCSEESE01_D: Social Engineering und Insider Threats .....	242
Kurs DLBCSEESE02_D: Projekt: Social Engineering .....	246

#### **Modul DLBCSEEHF\_E: Host Forensics**

Modulbeschreibung .....	249
Kurs DLBCSEEHF01_E: Static and Dynamic Malware Analysis .....	251
Kurs DLBCSEEHF02_E: Seminar: Sandbox Interpretation .....	254

#### **Modul DLBCSEEDSO\_D: DevSecOps**

Modulbeschreibung .....	257
Kurs IWNF01: Techniken und Methoden der agilen Softwareentwicklung .....	259
Kurs DLBCSEEDSO01_D: Projekt: Agiles DevSecOps-Software-Engineering .....	265

#### **Modul DLBCSEESCN\_D: Sicherheit in komplexen Netzwerken**

Modulbeschreibung .....	269
Kurs IAMG01: IT-Architekturmanagement .....	271
Kurs DLBCSEESCN01_D: Projekt: IT-Sicherheitsarchitekturen .....	275

#### **Modul DLBCSEENF\_E: Network Forensics**

Modulbeschreibung .....	279
Kurs DLBCSEENF01_E: Protocols, Log- and Dataflow-Analysis in Depth .....	281
Kurs DLBCSEENF02_E: Seminar: Threat Hunting, Analysis and Incident Response .....	284

### **6. Semester**

#### **Modul IWBI: Business Intelligence**

Modulbeschreibung .....	291
Kurs IWBI01: Business Intelligence .....	293
Kurs IWBI02: Projekt Business Intelligence .....	299

#### **Modul DLBCSEEF\_T\_D: Future Threats**

Modulbeschreibung .....	303
Kurs DLBCSEEF_T01_D: Threat Modeling .....	305
Kurs DLBCSEEF_T02_D: Projekt: Threat Modeling .....	309

#### **Modul DLBCSEEC\_S\_E: Cloud Security**

Modulbeschreibung .....	313
Kurs DLBCSEEC_S01_E: Security Controls in the Cloud .....	315
Kurs DLBCSEEC_S02_E: Project: Security by Design in the Cloud .....	319

#### **Modul DLBCSEEP\_T\_E: Pentesting**

Modulbeschreibung .....	321
Kurs DLBCSEEP_T01_E: Principles of Ethical Hacking .....	323

Kurs DLBCSEEPT02_E: Project: Pentesting .....	327
<b>Modul DLBCSEEIST_D: Industrielle Systemsicherheit</b>	
Modulbeschreibung .....	329
Kurs IGIS01: Grundlagen der industriellen Softwaretechnik .....	332
Kurs DLBCSEEIST01_D: Sicherheit im Internet of Things .....	338
<b>Modul DLBCSEECTI_E: Cyber Threat Intelligence</b>	
Modulbeschreibung .....	341
Kurs DLBCSEECTI01_E: Attack Models and Threat Feeds .....	344
Kurs DLBCSEECTI02_E: Project: Defense against APTs .....	348
<b>Modul DLBCSEEMT_D: Telekommunikationspezifische Bedrohungen</b>	
Modulbeschreibung .....	351
Kurs DLBCSEEMT01_D: Funk- und Telekommunikationssicherheit .....	354
Kurs DLBCSEEMT02_D: Softwarearchitektur mobiler Geräte .....	358
<b>Modul DLAMSD: Apple Mobile Solution Development</b>	
Modulbeschreibung .....	363
Kurs DLAMSD01: Apple Mobile Solution Development I .....	366
Kurs DLAMSD02: Apple Mobile Solution Development II .....	370
<b>Modul DLBCSEEISC_D: IT-Sicherheitsberatung</b>	
Modulbeschreibung .....	375
Kurs DLBCSEEISC01_D: Technische und betriebliche IT-Sicherheitskonzeptionen .....	378
Kurs DLBCSEEISC02_D: Projekt: Einsatz und Konfiguration von SIEM-Systemen .....	382
<b>Modul DLBCSEESE_D: Social Engineering</b>	
Modulbeschreibung .....	385
Kurs DLBCSEESE01_D: Social Engineering und Insider Threats .....	388
Kurs DLBCSEESE02_D: Projekt: Social Engineering .....	392
<b>Modul DLBCSEEHF_E: Host Forensics</b>	
Modulbeschreibung .....	395
Kurs DLBCSEEHF01_E: Static and Dynamic Malware Analysis .....	397
Kurs DLBCSEEHF02_E: Seminar: Sandbox Interpretation .....	400
<b>Modul DLBCSEEDSO_D: DevSecOps</b>	
Modulbeschreibung .....	403
Kurs IWNF01: Techniken und Methoden der agilen Softwareentwicklung .....	405
Kurs DLBCSEEDSO01_D: Projekt: Agiles DevSecOps-Software-Engineering .....	411
<b>Modul DLBCSEESCN_D: Sicherheit in komplexen Netzwerken</b>	
Modulbeschreibung .....	415
Kurs IAMG01: IT-Architekturmanagement .....	417

Kurs DLBCSEESC01_D: Projekt: IT-Sicherheitsarchitekturen .....	421
<b>Modul DLBCSEENF_E: Network Forensics</b>	
Modulbeschreibung .....	425
Kurs DLBCSEENF01_E: Protocols, Log- and Dataflow-Analysis in Depth .....	427
Kurs DLBCSEENF02_E: Seminar: Threat Hunting, Analysis and Incident Response .....	430
<b>Modul IWBI: Business Intelligence</b>	
Modulbeschreibung .....	433
Kurs IWBI01: Business Intelligence .....	435
Kurs IWBI02: Projekt Business Intelligence .....	441
<b>Modul DLBCSEEF0_D: Future Threats</b>	
Modulbeschreibung .....	445
Kurs DLBCSEEF01_D: Threat Modeling .....	447
Kurs DLBCSEEF02_D: Projekt: Threat Modeling .....	451
<b>Modul DLBCSEEC0_E: Cloud Security</b>	
Modulbeschreibung .....	455
Kurs DLBCSEEC01_E: Security Controls in the Cloud .....	457
Kurs DLBCSEEC02_E: Project: Security by Design in the Cloud .....	461
<b>Modul DLBCSEEP0_E: Pentesting</b>	
Modulbeschreibung .....	463
Kurs DLBCSEEP01_E: Principles of Ethical Hacking .....	465
Kurs DLBCSEEP02_E: Project: Pentesting .....	469
<b>Modul DLBCSEEI0_D: Industrielle Systemsicherheit</b>	
Modulbeschreibung .....	471
Kurs IGIS01: Grundlagen der industriellen Softwaretechnik .....	474
Kurs DLBCSEEI01_D: Sicherheit im Internet of Things .....	480
<b>Modul DLBCSEECTI_E: Cyber Threat Intelligence</b>	
Modulbeschreibung .....	483
Kurs DLBCSEECTI01_E: Attack Models and Threat Feeds .....	486
Kurs DLBCSEECTI02_E: Project: Defense against APTs .....	490
<b>Modul DLBCSEEMT_D: Telekommunikationspezifische Bedrohungen</b>	
Modulbeschreibung .....	493
Kurs DLBCSEEMT01_D: Funk- und Telekommunikationssicherheit .....	496
Kurs DLBCSEEMT02_D: Softwarearchitektur mobiler Geräte .....	500
<b>Modul BWSC: Supply Chain Management</b>	
Modulbeschreibung .....	505
Kurs BWSC01: Supply-Chain-Management I .....	508



Kurs BWSC02: Supply Chain Management II .....	514
<b>Modul DLBINGSF: Smart Factory</b>	
Modulbeschreibung .....	521
Kurs DLBINGSF01: Smart Factory I .....	524
Kurs DLBINGSF02: Smart Factory II .....	530
<b>Modul DLBCSDWRA: Robotics und Automatisierung</b>	
Modulbeschreibung .....	535
Kurs DLBINGFVI01: Fertigungsverfahren Industrie 4.0 .....	538
Kurs DLBINGAUR01: Automatisierung und Robotics .....	544
<b>Modul IWMB: Mobile Software Engineering</b>	
Modulbeschreibung .....	551
Kurs IWMB01: Mobile Software Engineering am Beispiel der Android-Plattform .....	553
Kurs IWMB02: Projekt Mobile Software Engineering .....	556
<b>Modul DLAMSD: Apple Mobile Solution Development</b>	
Modulbeschreibung .....	561
Kurs DLAMSD01: Apple Mobile Solution Development I .....	564
Kurs DLAMSD02: Apple Mobile Solution Development II .....	568
<b>Modul DLBSG: Studium Generale</b>	
Modulbeschreibung .....	573
Kurs DLBSG01: Studium Generale I .....	575
Kurs DLBSG02: Studium Generale II .....	579
<b>Modul BBAK: Bachelorarbeit</b>	
Modulbeschreibung .....	585
Kurs BBAK01: Bachelorarbeit .....	587
Kurs BBAK02: Kolloquium .....	592

---



# 1. Semester

---



# Betriebssysteme, Rechnernetze und verteilte Systeme

Modulcode: DLBIBRVS

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Dr. Frank Müller (Betriebssysteme, Rechnernetze und verteilte Systeme)

## Kurse im Modul

- Betriebssysteme, Rechnernetze und verteilte Systeme (DLBIBRVS01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: myStudium

Klausur, 90 Minuten

Studienformat: Kombistudium

Klausur, 90 Minuten

Studienformat: Fernstudium

Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

## Lehrinhalt des Moduls

- Betriebssysteme
- Rechnernetze
- Verteilte Systeme
- Mobile Computing

**Qualifikationsziele des Moduls****Betriebssysteme, Rechnernetze und verteilte Systeme**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Funktionen von Betriebssystemen zu erklären.
- verschiedene Betriebssysteme zu vergleichen.
- das OSI-Referenzmodell und den TCP/IP-Protokoll-Stack zu erläutern und zu vergleichen.
- die wichtigsten IP-basierten Protokolle und Dienste und deren Anwendung zu erläutern.
- unterschiedliche Architekturen für verteilte Systeme zu erläutern und zu vergleichen.
- die wichtigsten mobilen Kommunikationsnetze zu erläutern und zu vergleichen.
- grundlegende Herausforderungen und Lösungsansätze für Sicherheit im Internet zu erläutern.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Betriebssysteme, Rechnernetze und verteilte Systeme

Kurscode: DLBIBRVS01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Betriebssysteme sind eine zentrale Komponente von Rechnern und stellen grundlegende Funktionen für die Arbeit mit diesen Rechnern bereit. In immer größerem Maße stehen Rechner aber nicht alleine, sondern sind in Netzwerke eingebunden, innerhalb derer auf Daten und Funktionen anderer Computersysteme zugegriffen werden kann. Damit werden verteilte Systeme möglich, bei denen die Daten und Funktionen systematisch verschiedenen Rechnern innerhalb eines Netzwerkes zugeordnet werden, um gemeinsam definierte Aufgaben zu bewältigen. Während die verschiedenen Rechner innerhalb eines Netzwerkes oder eines verteilten Systems in der Vergangenheit stationär waren, sind mittlerweile auch viele mobile Rechner im Einsatz, was zu völlig neuen Anwendungsszenarien sowohl im privaten als auch im geschäftlichen Kontext führt.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Funktionen von Betriebssystemen zu erklären.
- verschiedene Betriebssysteme zu vergleichen.
- das OSI-Referenzmodell und den TCP/IP-Protokoll-Stack zu erläutern und zu vergleichen.
- die wichtigsten IP-basierten Protokolle und Dienste und deren Anwendung zu erläutern.
- unterschiedliche Architekturen für verteilte Systeme zu erläutern und zu vergleichen.
- die wichtigsten mobilen Kommunikationsnetze zu erläutern und zu vergleichen.
- grundlegende Herausforderungen und Lösungsansätze für Sicherheit im Internet zu erläutern.

## Kursinhalt

1. Grundlagen der Betriebssysteme
  - 1.1 Grundlegender Aufbau von Computersystemen
  - 1.2 Dateisysteme
  - 1.3 Speicherverwaltung
  - 1.4 Prozesse und Threads

2. Verbreitete Betriebssysteme
  - 2.1 Grundkonzepte Windows
  - 2.2 Grundkonzepte Unix und Linux
  - 2.3 Grundkonzepte Apple-Betriebssysteme
  - 2.4 Mobile Betriebssysteme
3. Rechnernetze
  - 3.1 Grundlagen der Datenübertragung
  - 3.2 OSI-Referenzmodell
  - 3.3 Netztopologien
4. TCP/IP und Internet
  - 4.1 Entstehung des Internets
  - 4.2 TCP/IP-Protokollstack
  - 4.3 Ausgewählte IP-basierte Protokolle und Dienste
  - 4.4 Sicherheit im Internet
5. Architekturen verteilter Systeme
  - 5.1 Client-Server-Systeme und verteilte Anwendungen
  - 5.2 Grundbegriffe verteilter Systeme: Nebenläufigkeit, Semaphoren, Deadlock
  - 5.3 Kommunikation in verteilten Systemen
  - 5.4 Dienste-Orientierung: SOA, Webservices und Microservices
  - 5.5 Cloud-Anwendungen
  - 5.6 Transaktionen in verteilten Systemen
  - 5.7 High-Performance Computing Cluster
6. Mobile Computing
  - 6.1 Grundlagen, Techniken und Protokolle für Mobile Computing
  - 6.2 Mobiles Internet und seine Anwendungen
  - 6.3 Mobile Kommunikationsnetze
  - 6.4 Sicherheit und Datenschutz in mobilen Systemen



**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Bengel, G. (2014): Grundkurs Verteilte Systeme. 4. Auflage. Vieweg+Teubner, Wiesbaden.
- Gumm H. P. /Sommer M. (2013): Einführung in die Informatik. 10. Auflage. Oldenbourg, München.
- Mandl, P. (2014): Grundkurs Betriebssysteme. 4. Auflage. Vieweg+Teubner, Wiesbaden.
- Schill, A./Springer, T. (2012): Verteilte Systeme. 2. Auflage. Springer Vieweg, Berlin Heidelberg.
- Tanenbaum, A.S./Bos, H. (2016): Moderne Betriebssysteme. 4. Auflage. Pearson Deutschland, Hallbergmoos.
- Tanenbaum, A.S./Wetherall, D.J. (2012): Computernetzwerke. 5. Auflage. Pearson Deutschland, Hallbergmoos.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	30 h	0 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# Einführung in Datenschutz und IT-Sicherheit

Modulcode: DLBINGEDS

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Ralf Kneuper (Einführung in Datenschutz und IT-Sicherheit)

## Kurse im Modul

- Einführung in Datenschutz und IT-Sicherheit (DLBISIC01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: myStudium

Klausur, 90 Minuten

Studienformat: Kombistudium

Klausur, 90 Minuten

Studienformat: Fernstudium

Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

## Lehrinhalt des Moduls

- Grundlagen der IT-Sicherheit
- Datenschutz
- IT-Sicherheitsmanagement
- Netzwerk- und Kommunikationssicherheit

**Qualifikationsziele des Moduls****Einführung in Datenschutz und IT-Sicherheit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Begriffe und Konzepte der IT-Sicherheit zu erläutern und typische Verfahren und Techniken zu benennen.
- gesetzliche Regelungen zum Datenschutz und ihre Umsetzung zu skizzieren.
- ihre vertieften Kenntnisse im Bereich IT-Sicherheitsmanagement sowie daraus abgeleitete, geeignete Maßnahmen in der Praxis umzusetzen.
- Aktivitäten und Strategien zur IT-Sicherheit in der Software- und Systementwicklung darzustellen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Einführung in Datenschutz und IT-Sicherheit

Kurscode: DLBISIC01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Die Studierenden lernen wichtige Konzepte aus dem Bereich IT-Sicherheit kennen. Dabei werden sowohl grundlegende Begriffe eingeführt und diskutiert als auch typische Anwendungsfelder und Einsatzgebiete von IT-Sicherheit vorgestellt sowie typische Verfahren und Techniken beschrieben.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Begriffe und Konzepte der IT-Sicherheit zu erläutern und typische Verfahren und Techniken zu benennen.
- gesetzliche Regelungen zum Datenschutz und ihre Umsetzung zu skizzieren.
- ihre vertieften Kenntnisse im Bereich IT-Sicherheitsmanagement sowie daraus abgeleitete, geeignete Maßnahmen in der Praxis umzusetzen.
- Aktivitäten und Strategien zur IT-Sicherheit in der Software- und Systementwicklung darzustellen.

## Kursinhalt

1. Begriffsbestimmungen und Hintergründe
  - 1.1 Informationstechnik (IT) für die Unterstützung von privaten Aktivitäten
  - 1.2 und geschäftlichen Prozessen
  - 1.3 Sicherheit und Schutz als Grundbedürfnisse
  - 1.4 Datenschutz als Persönlichkeitsrecht
  - 1.5 IT-Sicherheit als Qualitätsmerkmal von IT-Verbänden
  - 1.6 Abgrenzung Datenschutz und IT-Sicherheit
2. Grundlagen des Datenschutzes
  - 2.1 Prinzipien
  - 2.2 Rechtliche Vorgaben
  - 2.3 Informationelle Selbstbestimmung im Alltag

3. Grundlagen der IT-Sicherheit
  - 3.1 Paradigmen der IT-Sicherheit
  - 3.2 Modelle der IT-Sicherheit
  - 3.3 Rechtliche Vorgaben der IT-Sicherheit
4. Standards und Normen der IT-Sicherheit
  - 4.1 Grundlegende Standards und Normen
  - 4.2 Spezifische Standards und Normen
5. Erstellung eines IT-Sicherheitskonzeptes auf Basis von IT-Grundschutz
  - 5.1 Strukturanalyse
  - 5.2 Schutzbedarfsfeststellung
  - 5.3 Modellierung (Auswahl der Sicherheitsanforderungen)
  - 5.4 IT-Grundschutz-Check
  - 5.5 Risikoanalyse
6. Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte
  - 6.1 Schutz vor Diebstahl
  - 6.2 Schutz vor Schadsoftware (Malware)
  - 6.3 Sichere Anmeldeverfahren
  - 6.4 Sichere Speicherung von Daten
  - 6.5 Sichere Vernichtung von Daten
7. Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen
  - 7.1 Objektschutz
  - 7.2 Schutz vor unerlaubter Datenübertragung
  - 7.3 Schutz vor unerwünschtem Datenverkehr
  - 7.4 Schutz durch Notfallplanung



**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Harich, T. (2015): IT-Sicherheit im Unternehmen. Mitp, Frechen. 978-3958451285
- Kappes, M. (2013): Netzwerk- und Datensicherheit. Eine praktische Einführung. 2. Auflage, Springer Vieweg, Wiesbaden.
- Kersken, S. (2015): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 7. Auflage, Rheinwerk, Bonn.
- Kneuper, R. (2021): Datenschutz für Softwareentwicklung und IT. Springer Vieweg, Wiesbaden.
- Willems, E. (2015): Cybergefahr: Wie wir uns gegen Cyber-Crime und Online-Terror wehren können. Springer Vieweg, Wiesbaden.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

## Mathematik: Analysis

Modulcode: DLBBIMD

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	BA	5	150 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

### Modulverantwortliche(r)

Prof. Dr. Nazli Andjic (Mathematik: Analysis)

### Kurse im Modul

- Mathematik: Analysis (DLBBIMD01)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Klausur, 90 Minuten

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

- Folgen und Reihen
- Funktionen und Umkehrfunktionen
- Differentialrechnung
- Integralrechnung

**Qualifikationsziele des Moduls****Mathematik: Analysis**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundbegriffe der Analysis zusammenzufassen.
- die Begriffe „Folgen“ und „Reihen“ zu veranschaulichen.
- den Funktionsbegriff zu erläutern und das Konzept der Umkehrfunktion zu verstehen.
- grundlegende Aussagen der Differential- und Integralrechnung erklären zu können.
- den Zusammenhang zwischen Differentiation und Integration zu erläutern.
- die Ableitung von höher-dimensionalen Funktionen zu beherrschen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für weitere Module im Bereich  
Methoden

**Bezüge zu anderen Studiengängen der  
Hochschule**

Alle Bachelor-Programme im Bereich Wirtschaft  
& Management

# Mathematik: Analysis

Kurscode: DLBBIMD01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Die Analysis ist eines der wesentlichen Grundlagenfächer der Mathematik. Ihrem Ursprung nach entwickelt, um Probleme der klassischen Mechanik mathematisch formulieren und lösen zu können, ist sie in ihrer heutigen rigorosen Form in zahlreichen Anwendungen in den Naturwissenschaften und der Technik nicht mehr wegzudenken. Dieses Modul zielt ab auf die Einführung des grundlegenden Handwerkzeugs aus der Differential- und Integralrechnung sowie der Erläuterung deren wechselseitiger Zusammenhänge. Darüber hinaus erfolgt eine Verallgemeinerung der Differentialrechnung auf mehrdimensionale Räume.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundbegriffe der Analysis zusammenzufassen.
- die Begriffe „Folgen“ und „Reihen“ zu veranschaulichen.
- den Funktionsbegriff zu erläutern und das Konzept der Umkehrfunktion zu verstehen.
- grundlegende Aussagen der Differential- und Integralrechnung erklären zu können.
- den Zusammenhang zwischen Differentiation und Integration zu erläutern.
- die Ableitung von höher-dimensionalen Funktionen zu beherrschen.

## Kursinhalt

1. Folgen und Reihen
  - 1.1 Folgen: Konvergenz und Monotonie
  - 1.2 Reihen: Definition und Konvergenz
  - 1.3 Besondere Folgen und Reihen
2. Funktionen und Umkehrfunktionen
  - 2.1 Funktionen und ihre Eigenschaften
  - 2.2 Exponential- und Logarithmusfunktionen
  - 2.3 Trigonometrische Funktionen

3. Differentialrechnung
  - 3.1 Erste Ableitung und Potenzregel
  - 3.2 Ableitungsregeln und höhere Ableitungen
  - 3.3 Taylorreihe und Taylorpolynom
  - 3.4 Kurvendiskussion
  - 3.5 Ausblick: partielle Ableitungen
4. Integralrechnung
  - 4.1 Das unbestimmte Integral und Integrationsregeln
  - 4.2 Das bestimmte Integral und der Hauptsatz der Differential- und Integralrechnung
  - 4.3 Volumen und Mantelfläche von Rotationskörpern sowie Bogenlänge
5. Differentialgleichungen
  - 5.1 Einführung und Grundbegriffe
  - 5.2 Lösung von linearen homogenen Differentialgleichungen erster Ordnung
  - 5.3 Lösung von linearen inhomogenen Differentialgleichungen erster Ordnung
  - 5.4 Ausblick: partielle Differentialgleichungen

## Literatur

### Pfichtliteratur

### Weiterführende Literatur

- Arens, T. et al. (2013): Grundwissen Mathematikstudium. Analysis und Lineare Algebra mit Querverbindungen. Springer, Berlin/Heidelberg.
- Boas, M. L. (2006): Mathematical methods in the physical sciences. Third edition. Wiley. Hoboken, NJ.
- Deisenroth, M. P./Faisal, A./Ong C.-S. (2020): Math for ML. Cambridge University Press.
- Heuser, H. (2009): Lehrbuch der Analysis. Vieweg + Teubner (Studium). Wiesbaden.
- Modler, F./Kreh, M. (2014): Tutorium Analysis 1 und Lineare Algebra 1. Mathematik von Studenten für Studenten erklärt und kommentiert. 3. Auflage, Springer Spektrum, Berlin/Heidelberg.
- Papula, L. (2014): Mathematik für Ingenieure und Naturwissenschaftler. Bd. 1. Ein Lehr- und Arbeitsbuch für das Grundstudium. Springer Vieweg, Wiesbaden.



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input checked="" type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBBIMD01

## Einführung in das wissenschaftliche Arbeiten für IT und Technik

Modulcode: DLBWIRITT

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	BA	5	150 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

### Modulverantwortliche(r)

Prof. Dr. Amir Al-Munajjed (Einführung in das wissenschaftliche Arbeiten für IT und Technik)

### Kurse im Modul

- Einführung in das wissenschaftliche Arbeiten für IT und Technik (DLBWIRITT01)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: myStudium

*Prüfungsart*

Studienformat: Fernstudium

Advanced Workbook

Studienformat: Kombistudium

Advanced Workbook

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls**

- Alltagswissen vs. wissenschaftliches Arbeiten
- Das wissenschaftliche Arbeiten
- Umgang mit Quellen und Literatur
- Forschungsdesign
- Eine wissenschaftliche Arbeit schreiben
- Wissenschaftliches Arbeiten in IT und Technik in der Praxis

**Qualifikationsziele des Moduls****Einführung in das wissenschaftliche Arbeiten für IT und Technik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- zu erklären, was Wissenschaft ist und warum Wissenschaft benötigt wird (auch im praxisorientierten Studium und in der Berufspraxis).
- Theorien, Methoden und Modelle im Bereich IT und Technik zu benennen und anzuwenden.
- wissenschaftliche Literatur und Quellenarten zu finden, zu analysieren und einzuordnen.
- wissenschaftliche Arbeiten eigenständig anzufertigen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Methoden

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich Wirtschaft & Management

# Einführung in das wissenschaftliche Arbeiten für IT und Technik

Kurscode: DLBWIRITT01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Als Forschende und Studierende wollen wir Argumente nicht einfach für wahr halten, weil sie interessant klingen, sondern ihnen systematisch auf den Grund gehen. Dazu müssen wir wissenschaftlich denken. Aber was genau ist Wissenschaft? Der Kurs vermittelt die Grundlagen des wissenschaftlichen Denkens und Arbeitens und zeigt anhand konkreter Beispiele aus dem Bereich IT und Technik, welche Standards wissenschaftliche Arbeiten erfüllen müssen und wie sie aufgebaut sind. Studierende lernen wichtige Aspekte des wissenschaftlichen Arbeitens wie den Umgang mit Quellen, grundlegende Formate für Arbeiten in IT und Technik sowie die Methoden und Techniken, die nötig sind, um selbst wissenschaftliche Arbeiten an der IU zu schreiben.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- zu erklären, was Wissenschaft ist und warum Wissenschaft benötigt wird (auch im praxisorientierten Studium und in der Berufspraxis).
- Theorien, Methoden und Modelle im Bereich IT und Technik zu benennen und anzuwenden.
- wissenschaftliche Literatur und Quellenarten zu finden, zu analysieren und einzuordnen.
- wissenschaftliche Arbeiten eigenständig anzufertigen.

## Kursinhalt

1. Alltagswissen vs. wissenschaftliches Arbeiten
  - 1.1 Was ist wahr?
  - 1.2 Was sind vertrauenswürdige Quellen?
  - 1.3 Kritischer Umgang mit Primär- und Sekundärquellen
  - 1.4 Den eigenen Standpunkt entwickeln und argumentieren
  - 1.5 Aspekte wissenschaftlichen Arbeitens

2. Das wissenschaftliche Arbeiten
  - 2.1 Themenfindung
  - 2.2 Formate wissenschaftlicher Arbeiten
  - 2.3 Beispiel: Die Struktur einer wissenschaftlichen Arbeit
  - 2.4 Standards in IT und Technik
3. Umgang mit Quellen und Literatur
  - 3.1 Informationen beschaffen: Quellen und Literatur suchen, finden und bewerten
  - 3.2 Literaturverwaltung
  - 3.3 Wissenschaftliche Texte lesen
  - 3.4 Zitieren
  - 3.5 Plagiate vermeiden
4. Forschungsdesign
  - 4.1 Wichtige Formate
  - 4.2 Methoden: Quantitativ oder qualitativ?
  - 4.3 Methoden zur Datenerhebung
  - 4.4 Methoden zur Datenauswertung
  - 4.5 Ein Forschungsdesign wählen
5. Eine wissenschaftliche Arbeit schreiben
  - 5.1 Projekt- und Zeitplan
  - 5.2 Gliederung
  - 5.3 Format und Stil
  - 5.4 Ein wissenschaftliches Argument entwickeln
6. Wissenschaftliches Arbeiten in IT und Technik in der Praxis
  - 6.1 Mit Forschung zum Milliardär: Brin & Page, 1998
  - 6.2 Ein systematischer Literatur Review: Jansen-Preilowski et al., 2020
  - 6.3 Design Science Research: Kunzmann, 2022

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Benner-Wickner, M., Kneuper, R. & Schlömer, I. (2020). Leitfaden für die Nutzung von Design Science Research in Abschlussarbeiten.
- Heesen, B. (2021). Wissenschaftliches Arbeiten Methodenwissen für Wirtschafts-, Ingenieur- und Sozialwissenschaftler. Springer Gabler.
- Lindner, D. (2020). Forschungsdesigns der Wirtschaftsinformatik. Empfehlungen für die Bachelor- und Masterarbeit. Springer Gabler.
- Mayring, P. (2016). Einführung in die qualitative Sozialforschung: Eine Anleitung zu qualitativem Denken. Beltz.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b>
---------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Advanced Workbook

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Advanced Workbook

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien

# Einführung in die Programmierung mit Python

Modulcode: DLBDSIPWP\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Gabriele Bleser-Taetz (Einführung in die Programmierung mit Python)

## Kurse im Modul

- Einführung in die Programmierung mit Python (DLBDSIPWP01\_D)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Fernstudium  
Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

## Lehrinhalt des Moduls

- Python als Programmiersprache für Data Science
- Variablen und eingebaute Datentypen
- Aussagen und Funktionen
- Fehler- und Ausnahmebehandlung
- Wichtige Python-Daten-Wissenschaftsmodule

**Qualifikationsziele des Moduls****Einführung in die Programmierung mit Python**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Python-Syntax zu verwenden.
- gemeinsame elementare Datentypen zu erkennen.
- grundlegende Programmierkonzepte und ihre Umsetzung in Python zu erkennen.
- Fehlerbehandlung und –protokollierung zu verstehen.
- Arbeitsprogramme zu erstellen.
- die wichtigsten Bibliotheken und Pakete für die Datenwissenschaft aufzulisten.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module im Bereich Data Science & Artificial Intelligence

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Einführung in die Programmierung mit Python

Kurscode: DLBDSIPWP01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Dieser Kurs vermittelt den Teilnehmenden ein grundlegendes Verständnis der Programmiersprache Python. Nach einer einleitenden Darstellung der Bedeutung von Python für datenwissenschaftliche Programmieraufgaben werden die Studenten mit grundlegenden Programmierkonzepten wie Variablen, Datentypen und Anweisungen vertraut gemacht. Darauf aufbauend wird der wichtige Begriff einer Funktion erläutert und Fehler, Ausnahmebehandlung und Protokollierung erklärt. Der Kurs schließt mit einem Überblick über die am weitesten verbreiteten Bibliothekspakete für Data Science ab.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Python-Syntax zu verwenden.
- gemeinsame elementare Datentypen zu erkennen.
- grundlegende Programmierkonzepte und ihre Umsetzung in Python zu erkennen.
- Fehlerbehandlung und -protokollierung zu verstehen.
- Arbeitsprogramme zu erstellen.
- die wichtigsten Bibliotheken und Pakete für die Datenwissenschaft aufzulisten.

## Kursinhalt

1. Einführung
  - 1.1 Warum Python?
  - 1.2 Beschaffung und Installation von Python
  - 1.3 Der Python-Interpreter, IPython und Jupyter
2. Variablen und Datentypen
  - 2.1 Variablen und Wertzuweisung
  - 2.2 Zahlen
  - 2.3 Strings
  - 2.4 Sammlungen
  - 2.5 Dateien

3. Erklärungen
  - 3.1 Zuweisung, Ausdrücke und Druck
  - 3.2 Bedingte Anweisungen
  - 3.3 Schleifen
  - 3.4 Iteratoren und Verständnisse
4. Funktionen
  - 4.1 Funktionserklärung
  - 4.2 Umfang
  - 4.3 Argumente
5. Fehler und Ausnahmen
  - 5.1 Fehler
  - 5.2 Behandlung von Ausnahmen
  - 5.3 Protokolle
6. Module und Pakete
  - 6.1 Verwendung
  - 6.2 Namensräume
  - 6.3 Dokumentation
  - 6.4 Populäre Datenwissenschaftspakete

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Barry, P. (2016). Head First Python: A Brain-Friendly Guide (2. Aufl.). O'Reilly.
- Ernesti, J. & Kaiser, P. (2020). Python 3. Das umfassende Handbuch (6. Aufl.). Rheinwerk Computing.
- Mark, L. (2013). Learning Python: Powerful Object-Oriented Programming (5. Aufl.). O'Reilly.
- Steyer, R. (2018). Programmierung in Python. Ein kompakter Einstieg für die Praxis. SpringerVieweg.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBDSIPWP01\_D



## Statistik - Wahrscheinlichkeit und deskriptive Statistik

Modulcode: DLBDSSPDS\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof. Dr. Robert Graf (Statistik - Wahrscheinlichkeit und deskriptive Statistik)

### Kurse im Modul

- Statistik - Wahrscheinlichkeit und deskriptive Statistik (DLBDSSPDS01\_D)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Klausur oder Advanced Workbook, 90 Minuten

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

- Wahrscheinlichkeitsrechnung
- Zufallsvariablen
- Gemeinsame Verteilungen
- Erwartungswert und Varianz
- Ungleichungen und Grenzwertsätze

**Qualifikationsziele des Moduls****Statistik - Wahrscheinlichkeit und deskriptive Statistik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Wahrscheinlichkeiten, Zufallsvariablen und Wahrscheinlichkeitsverteilungen zu definieren.
- das Konzept der Bayessche Statistik zu verstehen.
- die Definition von gemeinsamen und marginalen Verteilungen zu verstehen.
- Erwartungswerte und höhere Momente zu berechnen.
- wichtige (stochastische) Ungleichungen und Grenzwertsätze zu verstehen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Methoden

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich Wirtschaft & Management

# Statistik - Wahrscheinlichkeit und deskriptive Statistik

Kurscode: DLBDSSPDS01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Die Beschreibung, Analyse und Zusammenfassung von Daten bilden die Grundlagen für datengetriebene Analyse- und Vorhersagemethoden. Dieser Kurs behandelt die dafür notwendigen Grundlagen der Wahrscheinlichkeitsrechnung und der deskriptiven Statistik, beginnend mit einer formalen Definition von Wahrscheinlichkeiten und einer Einführung in die Bayessche Statistik. Anschließend werden Zufallsvariablen und Wahrscheinlichkeitsdichtefunktionen sowie das Konzept der gemeinsamen und marginalen Verteilungen diskutiert. Dabei wird insbesondere auf die Bedeutung verschiedener diskreter und kontinuierlicher Verteilungen und ihrer Anwendungen eingegangen. Die Charakterisierung von Verteilungen ist ein wichtiger Aspekt bei der Beschreibung des Verhaltens von Wahrscheinlichkeitsverteilungen. Die Studierenden lernen deshalb Erwartungswerte, Varianzen und Kovarianzen zu berechnen. Die Konzepte der algebraischen und zentralen Momente und momenterzeugenden Funktionen ergänzen die Charakterisierung von Wahrscheinlichkeitsverteilungen. Schließlich konzentriert sich dieser Kurs auf wichtige Ungleichungen und Grenzwertsätze, wie etwa das Gesetz der großen Zahlen oder den zentralen Grenzwertsatz.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Wahrscheinlichkeiten, Zufallsvariablen und Wahrscheinlichkeitsverteilungen zu definieren.
- das Konzept der Bayessche Statistik zu verstehen.
- die Definition von gemeinsamen und marginalen Verteilungen zu verstehen.
- Erwartungswerte und höhere Momente zu berechnen.
- wichtige (stochastische) Ungleichungen und Grenzwertsätze zu verstehen.

## Kursinhalt

1. Wahrscheinlichkeitsrechnung
  - 1.1 Definitionen
  - 1.2 Unabhängige Ereignisse
  - 1.3 Bedingte Wahrscheinlichkeiten
  - 1.4 Bayessche Statistik

2. Zufallsvariablen
  - 2.1 Zufallsvariablen
  - 2.2 Verteilungsfunktionen und Wahrscheinlichkeitsfunktionen
  - 2.3 Wichtige diskrete Wahrscheinlichkeitsverteilungen
  - 2.4 Wichtige kontinuierliche Wahrscheinlichkeitsverteilungen
3. Gemeinsame Verteilungen
  - 3.1 Gemeinsame Verteilungen
  - 3.2 Randverteilungen
  - 3.3 Unabhängige Zufallsvariablen
  - 3.4 Bedingte Verteilungen
4. Erwartungswert und Varianz
  - 4.1 Erwartungswert einer Zufallsvariablen, bedingter Erwartungswert
  - 4.2 Varianz und Kovarianz
  - 4.3 Erwartungswerte und Varianzen wichtiger Wahrscheinlichkeitsverteilungen
  - 4.4 Algebraische und zentrale Momente
  - 4.5 Momenterzeugende Funktionen
5. Ungleichheiten und Grenzwertsätze
  - 5.1 Wahrscheinlichkeitsungleichheiten
  - 5.2 Ungleichheiten und Erwartungswerte
  - 5.3 Das Gesetz der großen Zahlen
  - 5.4 Zentraler Grenzwertsatz

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Arrenberg, J. (2020). Wirtschaftsstatistik für Bachelor (4. Aufl.). Utb.
- Arrenberg, J. (2021). Wirtschaftsstatistik: 77 Aufgaben, die Bachelorstudierende beherrschenmüssen (2. Aufl.). Utb.
- Bamberg, G., Baur, F. & Krapp, M. (2017). Statistik: eine Einführung für Wirtschafts- und Sozialwissenschaftler (18. Aufl.). De Gruyter Studium.
- Mathai, A. M. & Haubold, H. J. (2018). Probability and Statistics: a Course for Physicists and Engineers. De Gruyter.
- Wewel, M. C. & Blatter, A. (2019). Statistik im Bachelor-Studium der BWL und VWL: Methoden, Anwendung, Interpretation (4. Aufl.). Pearson Studium.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Advanced Workbook, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
100 h	0 h	25 h	25 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input checked="" type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBDSSPDS01\_D







## 2. Semester

---



# Grundlagen der objektorientierten Programmierung mit Java

Modulcode: DLBINGOPJ

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	BA	5	150 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

Prof. Dr. Damir Ismailovic (Grundlagen der objektorientierten Programmierung mit Java)

## Kurse im Modul

- Grundlagen der objektorientierten Programmierung mit Java (IOBP01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Kombistudium

Klausur, 90 Minuten

Studienformat: myStudium

Klausur, 90 Minuten

Studienformat: Fernstudium

Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls**

- Einführung in die Sprache Java
- Java-Sprachkonstrukte
- Einführung in die objektorientierte Systementwicklung
- Vererbung
- Objektorientierte Konzepte
- Ausnahmebehandlung
- Interfaces

**Qualifikationsziele des Moduls****Grundlagen der objektorientierten Programmierung mit Java**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundkonzepte der objektorientierten Modellierung und Programmierung zu erläutern und sie voneinander abzugrenzen.
- die Grundkonzepte und -elemente der Programmiersprache Java zu beschreiben und haben Erfahrungen in deren Verwendung.
- konkret beschriebene Probleme selbstständig zu lösen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Grundlagen der objektorientierten Programmierung mit Java

Kurscode: IOBP01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Betriebliche Informationssysteme werden in der Regel objektorientiert geplant und programmiert. Daher werden in diesem Kurs grundlegende Kompetenzen der objektorientierten Programmierung vermittelt. Dabei werden die theoretischen Konzepte unmittelbar anhand der Programmiersprache Java gezeigt und geübt.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundkonzepte der objektorientierten Modellierung und Programmierung zu erläutern und sie voneinander abzugrenzen.
- die Grundkonzepte und -elemente der Programmiersprache Java zu beschreiben und haben Erfahrungen in deren Verwendung.
- konkret beschriebene Probleme selbstständig zu lösen.

## Kursinhalt

1. Einführung in die objektorientierte Systementwicklung
  - 1.1 Objektorientierung als Sichtweise auf komplexe Systeme
  - 1.2 Das Objekt als Grundkonzept der Objektorientierung
  - 1.3 Phasen im objektorientierten Entwicklungsprozess
  - 1.4 Grundprinzip der objektorientierten Systementwicklung
2. Einführung in die objektorientierte Modellierung
  - 2.1 Strukturieren von Problemen mit Klassen
  - 2.2 Identifizieren von Klassen
  - 2.3 Attribute als Eigenschaften von Klassen
  - 2.4 Methoden als Funktionen von Klassen
  - 2.5 Beziehungen zwischen Klassen
  - 2.6 Unified Modeling Language (UML)

3. Programmieren von Klassen in Java
  - 3.1 Einführung in die Programmiersprache Java
  - 3.2 Grundelemente einer Klasse in Java
  - 3.3 Attribute in Java
  - 3.4 Methoden in Java
  - 3.5 main-Methode: Startpunkt eines Java-Programms
4. Java Sprachkonstrukte
  - 4.1 Primitive Datentypen
  - 4.2 Variablen
  - 4.3 Operatoren und Ausdrücke
  - 4.4 Kontrollstrukturen
  - 4.5 Pakete und Sichtbarkeitsmodifikatoren
5. Vererbung
  - 5.1 Modellierung von Vererbung im Klassendiagramm
  - 5.2 Programmieren von Vererbung in Java
6. Wichtige objektorientierte Konzepte
  - 6.1 Abstrakte Klassen
  - 6.2 Polymorphie
  - 6.3 Statische Attribute und Methoden
7. Konstruktoren zur Erzeugung von Objekten
  - 7.1 Der Standard-Konstruktor
  - 7.2 Überladen von Konstruktoren
8. Ausnahmebehandlung mit Exceptions
  - 8.1 Typische Szenarien der Ausnahmebehandlung
  - 8.2 Standard-Exceptions in Java
  - 8.3 Definieren eigener Exceptions
9. Programmierschnittstellen mit Interfaces
  - 9.1 Typische Szenarien für Programmierschnittstellen
  - 9.2 Interfaces als Programmierschnittstellen in Java

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Java (Hrsg.): Java Platform Standard Edition API Specification. (URL: <http://www.oracle.com/technetwork/java/api-141528.html> [letzter Zugriff: 21.11.2016]).
- Krüger G./Stark T. (2011): Handbuch der Java-Programmierung. 7. Auflage, Addison-Wesley, Salt Lake City.
- Lahres, B./Raýman, G. (2006): Praxisbuch Objektorientierung. Galileo Computing, Bonn.
- Oestereich B. (2012): Analyse und Design mit der UML 2.5. Objektorientierte Softwareentwicklung. 10. Auflage, Oldenbourg, München.
- Ratz, D. et al. (2011): Grundkurs Programmieren in Java. 6. Auflage, Carl Hanser Verlag, München.
- Ullenboom C. (2011): Java ist auch eine Insel. 10. Auflage, Galileo Computing, Bonn.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input checked="" type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input checked="" type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input checked="" type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# Mathematik: Lineare Algebra

Modulcode: DLBBIM

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	BA	5	150 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

Prof. Dr. Robert Graf (Mathematik: Lineare Algebra)

## Kurse im Modul

- Mathematik: Lineare Algebra (DLBBIM01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Kombistudium  
Klausur, 90 Minuten

Studienformat: Fernstudium  
Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

## Lehrinhalt des Moduls

- Matrix Algebra
- Vektor-Räume
- Lineare und affine Abbildungen
- Analytische Geometrie
- Matrix-Zerlegung

**Qualifikationsziele des Moduls****Mathematik: Lineare Algebra**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundbegriffe in Bezug auf lineare Gleichungssysteme zu erklären.
- Vektor-Räume und Eigenschaften von Vektoren zu veranschaulichen.
- Eigenschaften linearer und affiner Abbildungen zusammenzufassen.
- Zusammenhänge in der analytischen Geometrie darzustellen.
- verschiedene Methoden der Matrix-Zerlegung zu erkennen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für weitere Module im Bereich Methoden

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich Wirtschaft & Management

# Mathematik: Lineare Algebra

Kurscode: DLBBIM01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Die lineare Algebra stellt eines der Grundlagengebiete der Mathematik dar. Ihre historischen Ursprünge liegen in der Entwicklung von Lösungsmethoden für geometrische Probleme und – in engem Zusammenhang damit stehend – von linearen Gleichungssystemen. Es ist daher nicht verwunderlich, dass eine breite Vielzahl von physikalisch-technischen Anwendungsfragen mit ihrer Hilfe gelöst werden können. In diesem Kurs werden die Grundlagen der linearen Algebra herausgearbeitet, ihre Grundbegriffe wie Vektoren und Matrizen dargestellt und darauf aufbauend Lösungen für Problemstellungen der analytischen Geometrie hergeleitet.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundbegriffe in Bezug auf lineare Gleichungssysteme zu erklären.
- Vektor-Räume und Eigenschaften von Vektoren zu veranschaulichen.
- Eigenschaften linearer und affiner Abbildungen zusammenzufassen.
- Zusammenhänge in der analytischen Geometrie darzustellen.
- verschiedene Methoden der Matrix-Zerlegung zu erkennen.

## Kursinhalt

1. Grundlagen
  - 1.1 Lineare Gleichungssysteme
  - 1.2 Grundbegriffe zu Matrizen
  - 1.3 Matrix Algebra
  - 1.4 Matrizen als kompakte Repräsentation linearer Gleichungssysteme
  - 1.5 Inverse und Spur
2. Vektorräume
  - 2.1 Definition
  - 2.2 Linearkombination und lineare Abhängigkeit
  - 2.3 Basis, lineare Hülle und Rang

3. Lineare und affine Abbildungen
  - 3.1 Matrix-Repräsentation linearer Abbildungen
  - 3.2 Bild und Kern
  - 3.3 Affine Räume und Unter-Räume
  - 3.4 Affine Abbildungen
4. Analytische Geometrie
  - 4.1 Norm
  - 4.2 Skalarprodukt
  - 4.3 Orthogonale Projektionen
  - 4.4 Ausblick: Komplexe Zahlen
5. Matrix-Zerlegung
  - 5.1 Determinante
  - 5.2 Eigenwerte and Eigenvektoren
  - 5.3 Cholesky-Zerlegung
  - 5.4 Eigenwertzerlegung und Diagonalisierung
  - 5.5 Singulärwertzerlegung

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Arens, T. et al. (2022): Grundwissen Mathematikstudium. Analysis und Lineare Algebra mit Querverbindungen. 2. Auflage, Springer Spektrum, Berlin/Heidelberg.
- Deisenroth, M. P./Faisal, A./Ong C.-S. (2019): Mathematics for Machine Learning. Cambridge University Press, Cambridge. (Im Internet verfügbar).
- Dreiseitl, S. (2018): Mathematik für Software Engineering. Springer Vieweg, Berlin.
- Fischer, G. (2019): Lernbuch Lineare Algebra und Analytische Geometrie. 4. Auflage, Springer Spektrum, Wiesbaden.
- Lenze, B. (2020). Basiswissen Lineare Algebra : eine Einführung mit Aufgaben, Lösungen, Selbsttests und interaktivem Online-Tool. Springer Vieweg.
- Modler, F./Kreh, M. (2018): Tutorium Analysis 1 und Lineare Algebra 1. Mathematik von Studenten für Studenten erklärt und kommentiert. 4. Auflage, Springer Spektrum, Berlin/Heidelberg.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input checked="" type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input checked="" type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



## Kollaboratives Arbeiten

Modulcode: DLBKA

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof. Dr. Karin Halbritter (Kollaboratives Arbeiten)

### Kurse im Modul

- Kollaboratives Arbeiten (DLBKA01)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: myStudium

Fachpräsentation

Studienformat: Kombistudium

Fachpräsentation

Studienformat: Fernstudium

Fachpräsentation

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls**

- Selbstgesteuert und kollaborativ lernen
- Netzwerken und kooperieren
- Performance in (virtuellen) Teams
- Kommunizieren, argumentieren und überzeugen
- Konfliktpotenziale erkennen und Konflikte handhaben
- Selbstführung und Personal Skills

**Qualifikationsziele des Moduls****Kollaboratives Arbeiten**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die eigenen Lernprozesse selbstgesteuert und kollaborativ mit analogen und digitalen Medien zu gestalten.
- lokale und virtuelle Kooperation zu initiieren und geeignete Methoden zur Gestaltung der Zusammenarbeit auszuwählen.
- verschiedene Formen der Kommunikation in Bezug auf die Ziele und Erfordernisse unterschiedlicher Situationen zu beurteilen und das eigene Kommunikations- und Argumentationsverhalten zu reflektieren.
- Konfliktpotenziale und die Rolle von Emotionen bei Konflikten zu erläutern und den Einsatz von systemischen Methoden bei der ziel- und lösungsorientierten Handhabung von Konflikten zu beschreiben.
- die eigenen Ressourcen zu analysieren, Methoden der Selbstführung und -motivation darzustellen und angemessene Strategien abzuleiten.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Betriebswirtschaft & Management

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich Wirtschaft & Management

# Kollaboratives Arbeiten

Kurscode: DLBKA01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Der Kurs unterstützt die Studierenden darin, für unsere vernetzte Welt wichtige überfachliche Kompetenzen auf- und auszubauen – und dabei die Chancen einer konstruktiven Zusammenarbeit mit anderen zu nutzen. Er stellt wesentliche Formen und Gestaltungsmöglichkeiten von kollaborativem Lernen und Arbeiten vor, vermittelt grundlegende Kenntnisse und Werkzeuge für ein selbstgeführtes, flexibles und kreatives Denken, Lernen und Handeln und macht die Studierenden mit den Themen Empathiefähigkeit und emotionale Intelligenz vertraut. Zudem werden die Studierenden angeregt, die Kursinhalte anzuwenden. Damit fördern sie ihre autonome Handlungskompetenz sowie ihre Kompetenz in der interaktiven Anwendung von Tools und im Interagieren in heterogenen Gruppen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die eigenen Lernprozesse selbstgesteuert und kollaborativ mit analogen und digitalen Medien zu gestalten.
- lokale und virtuelle Kooperation zu initiieren und geeignete Methoden zur Gestaltung der Zusammenarbeit auszuwählen.
- verschiedene Formen der Kommunikation in Bezug auf die Ziele und Erfordernisse unterschiedlicher Situationen zu beurteilen und das eigene Kommunikations- und Argumentationsverhalten zu reflektieren.
- Konfliktpotenziale und die Rolle von Emotionen bei Konflikten zu erläutern und den Einsatz von systemischen Methoden bei der ziel- und lösungsorientierten Handhabung von Konflikten zu beschreiben.
- die eigenen Ressourcen zu analysieren, Methoden der Selbstführung und -motivation darzustellen und angemessene Strategien abzuleiten.

## Kursinhalt

1. Lernen für eine vernetzte Welt – in einer vernetzten Welt
  - 1.1 Anforderungen und Chancen der VUCA-Welt
  - 1.2 Lernen, Informationen und der Umgang mit Wissen und Nichtwissen
  - 1.3 4C-Modell: Collective – Collaborative – Continuous – Connected
  - 1.4 Eigenes Lernverhalten überprüfen

2. Networking & Kooperation
  - 2.1 Die passenden Kooperationspartner finden und gewinnen
  - 2.2 Tragfähige Beziehungen: Digital Interaction und Vertrauensaufbau
  - 2.3 Zusammenarbeit – lokal und virtuell organisieren & Medien einsetzen
  - 2.4 Social Learning: Lernprozesse agil, kollaborativ und mobil planen
3. Performance in (virtuellen) Teams
  - 3.1 Ziele, Rollen, Organisation und Performance Measurement
  - 3.2 Team Building und Team Flow
  - 3.3 Scrum als Rahmen für agiles Projektmanagement
  - 3.4 Design Thinking, Kanban, Planning Poker, Working-in-Progress-Limits & Co
4. Kommunizieren und überzeugen
  - 4.1 Kommunikation als soziale Interaktion
  - 4.2 Sprache, Bilder, Metaphern und Geschichten
  - 4.3 Die Haltung macht's: offen, empathisch und wertschätzend kommunizieren
  - 4.4 Aktiv zuhören – argumentieren – überzeugen – motivieren
  - 4.5 Die eigene Gesprächs- und Argumentationsführung analysieren
5. Konfliktpotenziale erkennen – Konflikte handhaben – wirksam verhandeln
  - 5.1 Vielfalt respektieren – Chancen nutzen
  - 5.2 Empathie für sich und andere entwickeln
  - 5.3 Systemische Lösungsarbeit und Reframing
  - 5.4 Konstruktiv verhandeln: klare Worte finden – Interessen statt Positionen
6. Eigene Projekte realisieren
  - 6.1 Wirksam Ziele setzen – fokussieren – reflektieren
  - 6.2 Vom agilen Umgang mit der eigenen Zeit
  - 6.3 (Selbst-)Coaching und Inneres Team
  - 6.4 Strategien und Methoden der Selbstführung und -motivation
7. Eigene Ressourcen mobilisieren
  - 7.1 Ressourcen erkennen – Emotionen regulieren
  - 7.2 Reflexion und Innovation – laterales Denken und Kreativität
  - 7.3 Transferstärke und Willenskraft: Bedingungsfaktoren analysieren und steuern

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Baber, A. (2015): Strategic connections. The new face of networking in a collaborative world. Amacom, New York.
- Burow, O.-A. (2015): Team-Flow. Gemeinsam wachsen im Kreativen Feld. Beltz, Weilheim/Basel.
- Goleman, D. (2013): Focus. The hidden driver of excellence. Harper Collins USA, New York.
- Grote, S./Goyk, R. (Hrsg.) (2018): Führungsinstrumente aus dem Silicon Valley. Konzepte und Kompetenzen. Springer Gabler, Berlin.
- Kaats, E./Opheij, W. (2014): Creating conditions for promising collaboration. Alliances, networks, chains, strategic partnerships. Springer Management, Berlin.
- Lang, M. D. (2019): The guide to reflective practice in conflict resolution. Rowman & Littlefield, Lanham/Maryland.
- Martin, S. J./Goldstein, N. J./Cialdini, R. B. (2015): The small BIG. Small changes that spark BIG influence. Profile Books, London.
- Parianen, F. (2017): Woher soll ich wissen, was ich denke, bevor ich höre, was ich sage? Die Hirnforschung entdeckt die großen Fragen des Zusammenlebens. Rowohlt Taschenbuch Verlag (Rowohlt Polaris), Reinbek bei Hamburg.
- Sauter, R./Sauter, W./Wolfig, R. (2018): Agile Werte- und Kompetenzentwicklung. Wege in eine neue Arbeitswelt. Springer Gabler, Berlin.
- Werther, S./Bruckner, L. (Hrsg.) (2018): Arbeit 4.0 aktiv gestalten. Die Zukunft der Arbeit zwischen Agilität, People Analytics und Digitalisierung. Springer Gabler, Berlin.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Fachpräsentation

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Fachpräsentation

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Fachpräsentation

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



# Einführung in die Netzwerkforensik

Modulcode: DLBCSEINF\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> DLBIBRVS01 oder DLBIBRVS01_E	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Dr. Andreas Schmidt (Einführung in die Netzwerkforensik)

## Kurse im Modul

- Einführung in die Netzwerkforensik (DLBCSEINF01\_D)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Fernstudium  
Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

## Lehrinhalt des Moduls

- Netzwerkprotokolle und -dienste
- World Wide Web
- Analyse von Protokolldaten
- Netzwerk-Forensik

**Qualifikationsziele des Moduls****Einführung in die Netzwerkforensik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- mit einem Netzwerk auf den unteren Netzwerkschichten zu interagieren.
- die Eigenheiten der Internetprotokolle zu verstehen.
- zu verstehen, wie man im Selbststudium Änderungen zur RFC Dokumentation bei der Modifikation oder Ergänzung von Protokollen lesen kann.
- allgemeine Angriffe geben dies Protokolle zu verstehen.
- zu verstehen wie Verschlüsselung im Internet genutzt wird und wie diese untergraben werden kann.
- IDPS Systeme einzusetzen und zu nutzen.
- Sicherheitsereignisse in SIEM, die IDPS Daten Nutzen zu erkennen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung.

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik.

# Einführung in die Netzwerkforensik

Kurscode: DLBCSEINF01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBIBRVS01 oder DLBIBRVS01_E

## Beschreibung des Kurses

Netzwerk-Forensik ist die Kunst und Wissenschaft der Erfassung, Aufzeichnung und Analyse von Netzwerkereignissen, um Angriffe aufzudecken. Dies erfordert eine vertiefte Kenntnis der wichtigsten Internet-Protokolle, wie sie verwendet werden und wie sie angegriffen werden können. In diesem Kurs werden wir uns mit den am häufigsten verwendeten Netzwerkprotokollen in internetbasierten Vernetzung befassen. Wir verfolgen einen praktischen Ansatz und betrachten aktuelle Netzwerkpuren, um herauszufinden, wie sich die Protokolle zueinander verhalten und aufeinander aufbauen. Im Kern geht es um TCP/IP. Andere Protokolle, wie HTTP, sind auf dieser Schicht aufgebaut. Andere, wie DNS, basieren auf dem alternativen UDP-Protokoll. Die wichtigsten Dienste, die das Internet ausmachen, werden diskutiert. Zum Beispiel ist DNS ein Protokoll, aber auch ein verteiltes Datenbanksystem. Die ICANN-Organisation überwacht die IP-Adressen, und sie werden an regionale Organisationen verteilt die dies an autonome Systeme weiter vergibt. Dies erfordert ein Routing, das von anderen Protokollen abgewickelt wird. Die Verschlüsselung erfolgt aus Gründen der Vertraulichkeit der Daten, aber oft auch aus Gründen der Authentifizierung und Integrität. Sie wird in einer Vielzahl von Formen mit ebenso vielfältigen Austauschbeziehungen implementiert. Der Forensik Experte benötigt eine Vielzahl von Werkzeugen, die von einfachen Sondierungswerkzeugen bis hin zu Erhebungs- und Analysewerkzeugen reichen. Diese werden in der Regel als „Intrusion Detection and Prevention“ Systeme sowie als SIEMs für die eigentliche Analyse zusammengefasst. Daten zu Sicherheitsereignissen müssen jedoch in der Regel mit externen Datenquellen für eine genaue Diagnose ergänzt werden, und es wird eine Vielzahl von Datenquellen diskutiert.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- mit einem Netzwerk auf den unteren Netzwerkschichten zu interagieren.
- die Eigenheiten der Internetprotokolle zu verstehen.
- zu verstehen, wie man im Selbststudium Änderungen zur RFC Dokumentation bei der Modifikation oder Ergänzung von Protokollen lesen kann.
- allgemeine Angriffe geben dies Protokolle zu verstehen.
- zu verstehen wie Verschlüsselung im Internet genutzt wird und wie diese untergraben werden kann.
- IDPS Systeme einzusetzen und zu nutzen.
- Sicherheitsereignisse in SIEM, die IDPS Daten Nutzen zu erkennen.

**Kursinhalt**

1. Warum Netzwerk-Forensik?
  - 1.1 Ziele der Untersuchungen
  - 1.2 Beweiserhebung im Netzwerk
  - 1.3 Erkennung von Eindringlingen
  - 1.4 (D)Dos-Erkennung und Entschärfung
  - 1.5 Marktverfügbare Werkzeuge
2. Grundlegende Protokoll-Schichtung
  - 2.1 Internet-Protokoll-Hierarchie
  - 2.2 Verbindung und verbindungslose Protokolle
  - 2.3 Lesen von RFCs und zugehöriger Dokumentation
3. TCP vs. UDP
  - 3.1 Verbindungsloses UDP
  - 3.2 TCP-Verbindungsaufbau
  - 3.3 Fehlende Pakete und Weiterleitung
  - 3.4 SOCKS-Proxying
  - 3.5 Angriffe gegen TCP und UDP
4. Das Internet-Protokoll
  - 4.1 IP-Adressen, IPv4 und IPv6
  - 4.2 Erlangen einer IPv4- und IPv6-Adresse
  - 4.3 Die Rolle der ICANN
  - 4.4 IP-Firewalls und Übersetzung von IP-Netzwerkadressen
  - 4.5 SOCKS-Proxying
5. Routing des Link-Layers
  - 5.1 ARP (Adressauflösungsprotokoll)
  - 5.2 Dynamisches RIP-Routing
  - 5.3 BGP-Peering
  - 5.4 Autonome Systemnummern
  - 5.5 Angriffe gegen Routing

6. Domänennamen-System
  - 6.1 Hostnamen-Hierarchie
  - 6.2 DNS als verteilte Datenbank
  - 6.3 DNSSEC
  - 6.4 SPF, DMARC und andere Sonderaufzeichnungen
7. Gemeinsame Protokolle der Anwendungs-Schicht
  - 7.1 HTTP
  - 7.2 HTTP/2
  - 7.3 SMTP
8. Transportschicht-Verschlüsselung
  - 8.1 SSH
  - 8.2 IPSEC
  - 8.3 TLS
  - 8.4 Man-In-The-Middle-Attack
  - 8.5 Zertifikate und Zertifizierungsstellen
9. Systeme zur Erkennung und Verhinderung von Eindringung
  - 9.1 Sensor- und Ereignistypen
  - 9.2 Netflow-Überwachung
  - 9.3 Regeln, falsch positive und falsch negative Ergebnisse
  - 9.4 SIEMs
  - 9.5 Technologien zur Angriffsvorbeugung
10. Korrelations- und Anreicherungsdatenquellen
  - 10.1 Anreicherung von Daten
  - 10.2 DNS-Datenquellen: DNSBLs, passives DNS, DNS-Repositorien
  - 10.3 AS-Nummern, IP-Blöcke, GeolP- und Whols-Daten
  - 10.4 Zertifikat-Transparenz
  - 10.5 Korrelationsmethoden

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Fall, K. R. / Stevens, W. R. (2012): TCP/IP Illustrated, Volume 1: The Protocols. 2nd edition, Addison-Wesley, Upper Saddle River, NJ.
- Matthews, J. (2005): Computer Networking: Internet Protocols in Action. Wiley, Hoboken, NJ.
- Stevens, W. R. (1996): TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols. Addison-Wesley, Upper Saddle River, NJ.
- Wright, G.R. / Stevens, W. R. (1995): TCP/IP Illustrated, Volume 2: The Implementation. Addison-Wesley, Upper Saddle River, NJ.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBCSEINF01\_D



# Requirements Engineering

Modulcode: IREN

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Tobias Brückmann (Requirements Engineering)

## Kurse im Modul

- Requirements Engineering (IREN01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: myStudium

Klausur, 90 Minuten

Studienformat: Fernstudium

Klausur, 90 Minuten

Studienformat: Kombistudium

Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls**

- Grundlagen des Requirements Engineering
- Unternehmensmodellierung
- Techniken der Anforderungsermittlung
- Techniken der Anforderungsdokumentation
- Prüfung und Abstimmung von Anforderungen
- Anforderungen verwalten

**Qualifikationsziele des Moduls****Requirements Engineering**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- mithilfe IT-Unterstützung relevanter Modelle eine Unternehmensmodellierung umzusetzen.
- Techniken und Methoden zu Ermittlung von Anforderungen an IT-Systeme voneinander abzugrenzen.
- Techniken zur Dokumentation von Anforderungen an IT-Systeme einzusetzen.
- Techniken zur Prüfung und Abstimmung sowie der Verwaltung von Anforderungen an IT-Systeme voneinander abzugrenzen.
- für gegebene Projektsituationen eigenständig geeignete Techniken und Methoden des Requirements Engineering auszuwählen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung.

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Requirements Engineering

Kurscode: IREN01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Die frühen Phasen der Softwareentwicklung sind maßgeblich davon gekennzeichnet, dass fachliche und technische Anforderungen (Requirements) an das IT-System zu ermitteln sind. Die Anforderungsermittlung muss äußerst umsichtig betrieben werden, weil alle folgenden Aktivitäten im SW-Entwicklungsprozess auf der Grundlage der dokumentierten Anforderungen geplant und durchgeführt werden. In diesem Kurs werden Vorgehensweisen, Methoden und Modelle vermittelt, die eine strukturierte und methodische Ermittlung und Dokumentation von Anforderungen an betriebliche Informationssysteme ermöglichen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- mithilfe IT-Unterstützung relevanter Modelle eine Unternehmensmodellierung umzusetzen.
- Techniken und Methoden zu Ermittlung von Anforderungen an IT-Systeme voneinander abzugrenzen.
- Techniken zur Dokumentation von Anforderungen an IT-Systeme einzusetzen.
- Techniken zur Prüfung und Abstimmung sowie der Verwaltung von Anforderungen an IT-Systeme voneinander abzugrenzen.
- für gegebene Projektsituationen eigenständig geeignete Techniken und Methoden des Requirements Engineering auszuwählen.

## Kursinhalt

1. Grundlagen und Begriffe des Requirements Engineering
  - 1.1 Requirements Engineering im Softwareprozess
  - 1.2 Kernaktivitäten im Requirements Engineering
  - 1.3 Was ist eine Anforderung?
2. Ermittlung von Anforderungen
  - 2.1 Bestimmung des Systemkontextes
  - 2.2 Bestimmung der Quellen von Anforderungen
  - 2.3 Ausw.hlen der geeigneten Ermittlungstechniken
  - 2.4 Anforderungen unter Einsatz der Techniken ermitteln

3. Ausgewählte Ermittlungstechniken
  - 3.1 Kreativitätstechniken
  - 3.2 Befragungstechniken
  - 3.3 Beobachtungstechniken
  - 3.4 Prototyping
4. Dokumentation von Anforderungen
  - 4.1 Aktivitäten zur Dokumentation von Anforderungen
  - 4.2 Typische Elemente der Anforderungsdokumentation
  - 4.3 Dokumentationsformen
5. Modellierung von Prozessen
  - 5.1 Grundlagen und Begriffe
  - 5.2 Modellierung mit der Business Process Model and Notation
  - 5.3 Modellierung mit Ereignisgesteuerten Prozessketten
6. Modellierung von Systemen
  - 6.1 Grundlagen Unified Modeling Language
  - 6.2 UML-Use Case-Diagramm
  - 6.3 UML-Aktivitätsdiagramm
  - 6.4 UML-Klassendiagramm
  - 6.5 UML-Zustandsdiagramm
7. Prüfen und Abstimmen von Anforderungen
  - 7.1 Aktivitäten zum Prüfen und Abstimmen von Anforderungen
  - 7.2 Prüfkriterien
  - 7.3 Prüfprinzipien
  - 7.4 Prüftechniken
  - 7.5 Abstimmen von Anforderungen
8. Management von Anforderungen und Techniken zur Priorisierung
  - 8.1 Verwalten von Anforderungen
  - 8.2 Techniken zur Priorisierung von Anforderungen

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Pohl, K./Rupp, C. (2021): Basiswissen Requirements Engineering – Aus- und Weiterbildung zum „Certified Professional for Requirements Engineering“. 5. Auflage, dpunkt.verlag, Heidelberg.
- Rupp, C./die SOPHISTen (2021): Requirements-Engineering und -Management: Aus der Praxis von klassisch bis agil. 7. Auflage, Carl Hanser, München.
- Rupp, C./die SOPHISTen/Queins, S. (2012): UML 2 glasklar: Praxiswissen für die UML-Modellierung. 4. Auflage, Carl Hanser, München.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



## Grundzüge des System-Pentestings

Modulcode: DLBCSESPB\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof. Dr. Stephan Spitz (Grundzüge des System-Pentestings)

### Kurse im Modul

- Grundzüge des System-Pentestings (DLBCSESPB01\_D)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Klausur, 90 Minuten

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

- Ablauf von Penetrationstests
- Host-basierte Penetrationstests
- Ausnutzung von Netzwerkdiensten
- Web-App-Penetrationstest
- Systemhärtung
- Ethisches Hacking

**Qualifikationsziele des Moduls****Grundzüge des System-Pentestings**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden organisatorischen und einzuhaltenden Anforderungen für Penetrationstests zu verstehen.
- die relevanten Komponenten eines modernen IT-Systems, welche nutzbar sein könnten, zu identifizieren.
- die grundlegenden Prozesse, die ein Penetrationstest umfasst, zu verstehen.
- die häufigsten Angriffsvektoren auf Hosts, Netzwerke und Web Apps verstehen und zu wissen, wie man sich gegen diese verteidigen kann.
- sich mit praxisnahen Werkzeugen vertraut zu machen, die von professionellen Penetrationstestern eingesetzt werden.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Grundzüge des System-Pentestings

Kurscode: DLBCSESPB01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

System-Penetrationstests sind ein wichtiger Prozess, um Schwachstellen in IT-Systemen zu finden und deren Behebung zu unterstützen, bevor Angreifer sie ausnutzen können. Aus diesem Grund setzen viele Organisationen solche "Pentester" oder ethische Hacker ein, um ihre Software- und Hardwarebasis (einschließlich Konnektivität) zu testen und die gefundenen Sicherheitsprobleme zu beheben. Dies ist zu einem Eckpfeiler moderner Sicherheitskonzepte geworden. Um bei diesem Unterfangen erfolgreich zu sein, ist jedoch eine gute Kenntnis der verschiedenen Arten von anvisierten IT-Systemen erforderlich. Wir beziehen uns auf Hosts, Netzwerke, Web Apps und sogar Cloud Computing. In diesem Kurs stellen wir die grundlegenden Aspekte von IT-Systemen sowie die Prozesse, Hilfsmittel und Techniken vor, die die industrielle Praxis der Penetrationstests ausmachen. Ausgerüstet mit diesem Wissen werden die Studierenden die Mechanismen eines bestimmten Angriffs verstehen und sich auf den Weg eigener Penetration Tests begeben.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden organisatorischen und einzuhaltenden Anforderungen für Penetrationstests zu verstehen.
- die relevanten Komponenten eines modernen IT-Systems, welche nutzbar sein könnten, zu identifizieren.
- die grundlegenden Prozesse, die ein Penetrationstest umfasst, zu verstehen.
- die häufigsten Angriffsvektoren auf Hosts, Netzwerke und Web Apps verstehen und zu wissen, wie man sich gegen diese verteidigen kann.
- sich mit praxisnahen Werkzeugen vertraut zu machen, die von professionellen Penetrationstestern eingesetzt werden.

## Kursinhalt

1. Ziele von Penetrationstests und industrielle Perspektive
  - 1.1 Organisatorischer Nutzen
  - 1.2 Rahmenbedingungen für Ethical Hacking
  - 1.3 Rechtliche Aspekte
  - 1.4 Verantwortungsvolle Offenlegung von Schwachstellen
  - 1.5 Professionelle Penetrationstest-Dienstleistungen und Zertifizierungen

2. Hintergrundkonzepte
  - 2.1 Betriebssysteme
  - 2.2 Hardware-Architekturen
  - 2.3 Netzwerke und Protokolle
  - 2.4 Web-basierte Anwendungen
  - 2.5 Cloud-Computing
3. Ablauf von Penetrationstests
  - 3.1 Planung und Erkundung
  - 3.2 Whitebox-, Blackbox- und Graybox-Scanning
  - 3.3 Zugang erhalten
  - 3.4 Aufrechterhaltung des Zugangs
  - 3.5 Analyse und Berichterstattung
  - 3.6 Härtung und Entschärfung
4. Betriebssystembasierte Penetrationstests
  - 4.1 Häufige Fehlkonfigurationen
  - 4.2 Shellcode-Angriffe
  - 4.3 Speicherkorruption und Pufferüberlauf-Schwachstellen
  - 4.4 Metasploit und Kali-Tools
  - 4.5 Härtung des Betriebssystems
5. Netzwerk-Penetrationstests
  - 5.1 Scoping und Recon der Netzwerkinfrastruktur
  - 5.2 Ausnutzen von Netzwerkdiensten
  - 5.3 Seitliche Bewegung im Netzwerk
  - 5.4 Kerberos-Angriffe
  - 5.5 Werkzeugsatz: Nmap, PowerShell, Bloodhound und Tcpdump
  - 5.6 Entwickeln von Korrekturmaßnahmen
6. Web-App-Penetrationstests
  - 6.1 Die OWASP-Methodik
  - 6.2 Open-Source-Intelligenz (OSINT)
  - 6.3 Häufig ausgenutzte Web-App-Schwachstellen
  - 6.4 Ausnutzungs-Toolset: BurpSuite, sqlmap, BeEF und ExploitDB
  - 6.5 Berichterstattung über Ergebnisse und Abhilfemaßnahmen

7. Spezialisierte Penetrationstests auf einen Blick
  - 7.1 Ausnutzungs-Entwicklung
  - 7.2 Ethisches Hacking
  - 7.3 Penetrationstests für drahtlose und mobile Geräte
  - 7.4 Bewertung von Cloud-Bedrohungen und Schwachstellen

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Amberg, E. & Schmid, D. (2022). Hacking. Der umfassende Praxis-Guide (2. Aufl.). mitp.
- Weidmann, G. (2014). Penetration testing: a hands-on introduction to hacking. No starch.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien







# 3. Semester

---



## Interkulturelle und ethische Handlungskompetenzen

Modulcode: DLBIHK

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof. Dr. Jürgen Matthias Seeler (Interkulturelle und ethische Handlungskompetenzen)

### Kurse im Modul

- Interkulturelle und ethische Handlungskompetenzen (DLBIHK01)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: myStudium  
Schriftliche Ausarbeitung: Fallstudie

Studienformat: Fernstudium  
Schriftliche Ausarbeitung: Fallstudie

Studienformat: Kombistudium  
Schriftliche Ausarbeitung: Fallstudie

#### Teilmodulprüfung

#### Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls**

- Grundlagen interkultureller Handlungskompetenz
- Kulturkonzepte
- Kultur und Ethik
- Implikationen aktueller ethischer Probleme im Bereich Interkulturalität, Ethik und Diversity
- Interkulturelles Lernen und Arbeiten
- Fallbeispiele für kulturelle und ethische Konflikte

**Qualifikationsziele des Moduls****Interkulturelle und ethische Handlungskompetenzen**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wichtigsten Begriffe in den Bereichen Interkulturalität, Diversity und Ethik zu erklären.
- unterschiedliche Erklärungsmuster von Kultur voneinander abzugrenzen.
- Kultur auf verschiedenen Ebenen zu begreifen.
- Prozesse interkulturellen Lernens und Arbeitens zu planen.
- die Interdependenzen von Kultur und Ethik zu verstehen.
- eine Fallstudie zur interkulturellen Handlungskompetenz selbständig zu bearbeiten.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Methoden

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich Wirtschaft & Management

# Interkulturelle und ethische Handlungskompetenzen

Kurscode: DLBIHK01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

In diesem Kurs erwerben die Studierenden das nötige Wissen, um interkulturelle Handlungskompetenzen sowie aktuelle Entwicklungen zu den Themen Diversity und Ethik zu verstehen. Die Studierenden verstehen, wie sie Lernprozesse zur Entwicklung der in diesen Bereichen wichtigen Kompetenzen systematisch planen und durchführen. Dazu werden zunächst wichtige Begriffe geklärt und voneinander abgegrenzt. Der Kulturaspekt wird aus verschiedenen Perspektiven erklärt. Zudem lernen Studierende, dass Kulturfragen auf unterschiedlichen Ebenen relevant sind, etwa innerhalb eines Staates, in einem Unternehmen und auch in jeder anderen Gruppe. In diesem Kontext erkennen die Studierenden auch den Zusammenhang zwischen Ethik und Kultur mit verschiedenen Interdependenzen. Auf der Grundlage dieses Wissens werden die Studierenden dann mit den unterschiedlichen Möglichkeiten und Potenzialen interkulturellen und ethischen Lernens und Arbeitens vertraut gemacht. Anhand von Praxisfällen werden die erlernten Zusammenhänge in ihrer Bedeutung für den heutigen Arbeitskontext in vielen Unternehmen deutlich gemacht. Die Studierenden bearbeiten sodann eine Fallstudie, in der das erworbene Wissen systematisch angewendet wird.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wichtigsten Begriffe in den Bereichen Interkulturalität, Diversity und Ethik zu erklären.
- unterschiedliche Erklärungsmuster von Kultur voneinander abzugrenzen.
- Kultur auf verschiedenen Ebenen zu begreifen.
- Prozesse interkulturellen Lernens und Arbeitens zu planen.
- die Interdependenzen von Kultur und Ethik zu verstehen.
- eine Fallstudie zur interkulturellen Handlungskompetenz selbständig zu bearbeiten.

## Kursinhalt

1. Grundlagen interkultureller und ethischer Handlungskompetenz
  - 1.1 Gegenstandsbereiche, Begriffe und Definitionen
  - 1.2 Relevanz interkulturellen und ethischen Handelns
  - 1.3 Interkulturelles Handeln – Diversity, Globalisierung, Ethik

2. Kulturkonzepte
  - 2.1 Hofstede's Kulturdimensionen
  - 2.2 Kulturdifferenzierung nach Hall
  - 2.3 Locus-of-Control-Konzept nach Rotter
3. Kultur und Ethik
  - 3.1 Ethik – Grundbegriffe und Konzepte
  - 3.2 Interdependenz von Kultur und Ethik
  - 3.3 Ethische Konzepte in verschiedenen Regionen der Welt
4. Aktuelle Themen im Bereich Interkulturalität, Ethik und Diversity
  - 4.1 Digital Ethics
  - 4.2 Gleichberechtigung und Gleichstellung
  - 4.3 Social Diversity
5. Interkulturelles Lernen und Arbeiten
  - 5.1 Akkulturation
  - 5.2 Lernen und Arbeiten in interkulturellen Arbeitsgruppen
  - 5.3 Strategien zum Umgang mit kulturell geprägten Konflikten
6. Fallbeispiele für kulturelle und ethische Konflikte
  - 6.1 Fallbeispiel Interkulturalität
  - 6.2 Fallbeispiel Diversity
  - 6.3 Fallbeispiel Interkulturalität und Ethik

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Emrich, C. (2011): Interkulturelles Management: Erfolgsfaktoren im globalen Business. Kohlhammer-Verlag, Stuttgart/Berlin/Köln.
- Erll, A./Gymnich, M. (2015): Uni-Wissen Interkulturelle Kompetenzen: Erfolgreich kommunizieren zwischen den Kulturen – Kernkompetenzen. 4. Auflage, Klett Lerntraining, Stuttgart.
- Eß, O. (2010): Das Andere lehren: Handbuch zur Lehre Interkultureller Handlungskompetenz. Waxmann Verlag, Münster.
- Hofstede, G./ Hofstede, G. J./Minkov, M. (2017): Lokales Denken, globales Handeln Interkulturelle Zusammenarbeit und globales Management. 6. Auflage, Beck, München.
- Leenen, W.R./Groß, A. (2018): Handbuch Methoden Interkultureller Bildung und Weiterbildung. Verlag Vandenhoeck & Ruprecht, Göttingen.
- Thomas, A. (2011): Interkulturelle Handlungskompetenz. Versiert, angemessen und erfolgreich im internationalen Geschäft. Gabler-Verlag, Wiesbaden.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

## Einführung in das Internet of Things

Modulcode: DLBINGEIT

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof. Dr. Marian Benner-Wickner (Einführung in das Internet of Things)

### Kurse im Modul

- Einführung in das Internet of Things (DLBINGEIT01)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Kombistudium  
Klausur oder Fachpräsentation, 90 Minuten

Studienformat: myStudium  
Klausur oder Fachpräsentation, 90 Minuten

Studienformat: Fernstudium  
Klausur oder Fachpräsentation, 90 Minuten

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

<p><b>Lehrinhalt des Moduls</b></p> <ul style="list-style-type: none"> <li>▪ Grundlagen des Internet of Things</li> <li>▪ Gesellschaftliche und wirtschaftliche Bedeutung</li> <li>▪ Kommunikationsstandards und -technologien</li> <li>▪ Datenspeicherung und -verarbeitung</li> <li>▪ Design und Entwicklung</li> <li>▪ Anwendungsbereiche</li> </ul>	
<p><b>Qualifikationsziele des Moduls</b></p> <p><b>Einführung in das Internet of Things</b></p> <p>Nach erfolgreichem Abschluss sind die Studierenden in der Lage,</p> <ul style="list-style-type: none"> <li>▪ die besonderen Eigenschaften des Internet of Things (IoT) und von IoT-Systemen zu erläutern.</li> <li>▪ die gesellschaftliche und wirtschaftliche Bedeutung des Internet of Things einzuschätzen.</li> <li>▪ die wichtigsten Standards für die Kommunikation zwischen IoT-Geräten wiederzugeben.</li> <li>▪ verschiedene Techniken zur Speicherung und Verarbeitung von Daten in IoT-Systemen zu kategorisieren.</li> <li>▪ verschiedene Architekturen und Technologien zur Strukturierung von IoT-Systemen zu erläutern.</li> <li>▪ die Herausforderungen des Datenschutzes und der Datensicherheit in IoT-Systemen einschätzen zu können.</li> </ul>	
<p><b>Bezüge zu anderen Modulen im Studiengang</b></p> <p>Ist Grundlage für alle weiteren Module aus dem Bereich Informatik &amp; Software-Entwicklung</p>	<p><b>Bezüge zu anderen Studiengängen der Hochschule</b></p> <p>Alle Bachelor-Programme im Bereich IT &amp; Technik</p>

# Einführung in das Internet of Things

Kurscode: DLBINGEIT01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen Einblick in die technischen und theoretischen Grundlagen des Internet of Things (IoT) und dessen Anwendungsgebiete zu bieten. Neben dem generellen Aufbau von IoT-Systemen und der darin eingesetzten Technologiestandards wird den Studenten auch die Bedeutung des Internet of Things für Wirtschaft und Gesellschaft vermittelt. Darüber hinaus wird dargestellt, auf welche Weise Daten im IoT ausgetauscht, gespeichert und verarbeitet werden.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die besonderen Eigenschaften des Internet of Things (IoT) und von IoT-Systemen zu erläutern.
- die gesellschaftliche und wirtschaftliche Bedeutung des Internet of Things einzuschätzen.
- die wichtigsten Standards für die Kommunikation zwischen IoT-Geräten wiederzugeben.
- verschiedene Techniken zur Speicherung und Verarbeitung von Daten in IoT-Systemen zu kategorisieren.
- verschiedene Architekturen und Technologien zur Strukturierung von IoT-Systemen zu erläutern.
- die Herausforderungen des Datenschutzes und der Datensicherheit in IoT-Systemen einschätzen zu können.

## Kursinhalt

1. Grundlagen des Internet of Things
  - 1.1 Das Internet der Dinge – Grundlagen und Motivation
  - 1.2 Evolution des Internets – Web 1.0 bis Web 4.0
2. Gesellschaftliche und wirtschaftliche Bedeutung
  - 2.1 Innovationen für Verbraucher und Industrie
  - 2.2 Auswirkungen auf Mensch und Arbeitswelt
  - 2.3 Datenschutz und Datensicherheit

3.	Kommunikationsstandards und -technologien
3.1	Netzwerktopologien
3.2	Netzwerkprotokolle
3.3	Technologien
4.	Datenspeicherung und -verarbeitung
4.1	Vernetztes Speichern mit Linked Data und RDF(S)
4.2	Analyse vernetzter Daten mit dem Semantic Reasoner
4.3	Verarbeitung von Datenströmen mit Complex Event Processing
4.4	Betrieb und Analyse großer Datenmengen mit NoSQL und MapReduce
5.	Design und Entwicklung
5.1	Software Engineering für verteilte und eingebettete Systeme
5.2	Architekturstile und -muster verteilter Systeme
5.3	Mikrocontroller
6.	Anwendungsbereiche
6.1	Smarthome/Smart Living
6.2	Ambient Assisted Living
6.3	Smart Energy/Smart Grid
6.4	Smart Factory
6.5	Smart Logistics

<b>Literatur</b>
<b>Pflichtliteratur</b>
<b>Weiterführende Literatur</b>
<ul style="list-style-type: none"> <li>▪ Andelfinger, V. P./Hänisch, T. (Hrsg.) (2015): Internet der Dinge. Technik, Trends und Geschäftsmodelle. Springer, Wiesbaden.</li> <li>▪ Buyya, R./Vahid Dastjerdi, A. (Hrsg.) (2016): Internet of things. Principles and paradigms. Morgan Kaufmann, Cambridge (MA).</li> <li>▪ Christoph, E./Sprenger, F. (Hrsg.) (2015): Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt. transcript, Bielefeld.</li> <li>▪ Fleisch, E. (Hrsg.) (2005): Internet der dinge. Ubiquitous Computing und RFID in der Praxis. Springer, Berlin.</li> <li>▪ Gilchrist, A. (2016): Industry 4.0. The industrial internet of things. Apress, New York.</li> <li>▪ Kaufmann, T. (2015): Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge. Der Weg vom Anspruch in die Wirklichkeit. Springer, Wiesbaden.</li> </ul>

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Fachpräsentation, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
100 h	0 h	25 h	25 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input checked="" type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Fachpräsentation, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
100 h	0 h	25 h	25 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input checked="" type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Fachpräsentation, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
100 h	0 h	25 h	25 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input checked="" type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBINGEIT01

# Algorithmen, Datenstrukturen und Programmiersprachen

Modulcode: DLBIADPS

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	IOBP01, DLBCSDSJCL02_D	BA	5	150 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

Johannes Kent Walter (Algorithmen, Datenstrukturen und Programmiersprachen)

## Kurse im Modul

- Algorithmen, Datenstrukturen und Programmiersprachen (DLBIADPS01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Fernstudium

Klausur, 90 Minuten

Studienformat: myStudium

Klausur, 90 Minuten

Studienformat: Kombistudium

Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

<p><b>Lehrinhalt des Moduls</b></p> <ul style="list-style-type: none"> <li>▪ Datenstrukturen</li> <li>▪ Algorithmen-Entwurf</li> <li>▪ Wichtige Algorithmen</li> <li>▪ Grundbegriffe XML</li> <li>▪ Programmierparadigmen und Grundbegriffe von Programmiersprachen</li> <li>▪ Überblick über verbreitete Programmiersprachen</li> </ul>	
<p><b>Qualifikationsziele des Moduls</b></p> <p><b>Algorithmen, Datenstrukturen und Programmiersprachen</b></p> <p>Nach erfolgreichem Abschluss sind die Studierenden in der Lage,</p> <ul style="list-style-type: none"> <li>▪ grundlegende Datenstrukturen zu erklären und in konkreten Anwendungsfällen zu vergleichen und anzuwenden.</li> <li>▪ grundlegende Algorithmen zu erklären.</li> <li>▪ in konkreten Anwendungsfällen geeignete Algorithmen zu entwerfen oder auszuwählen sowie anzuwenden.</li> <li>▪ den Einsatz XML als Datenstruktur sowie die wichtigsten Algorithmen und Konzepte zur Verarbeitung von XML-Dokumenten (DOM, SAX, XLS) zu erklären und in einfachen Anwendungsfällen anzuwenden.</li> <li>▪ die verbreiteten Programmierparadigmen und Programmiersprachen zu erläutern und zu vergleichen.</li> </ul>	
<p><b>Bezüge zu anderen Modulen im Studiengang</b></p> <p>Ist Grundlage für alle weiteren Module aus dem Bereich Informatik &amp; Software-Entwicklung.</p>	<p><b>Bezüge zu anderen Studiengängen der Hochschule</b></p> <p>Alle Bachelor-Programme im Bereich IT &amp; Technik</p>

# Algorithmen, Datenstrukturen und Programmiersprachen

Kurscode: DLBIADPS01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IOBP01, DLBCSDSJCL02_D

## Beschreibung des Kurses

Programmierung besteht im Wesentlichen daraus, für eine konkrete Aufgabenstellung geeignete Algorithmen und Datenstrukturen auszuwählen und diese in Programmcode umzusetzen. Dabei gibt es eine Vielzahl unterschiedlicher Programmiersprachen, die auf unterschiedlichen Vorgehensweisen beruhen und in denen Algorithmen und Datenstrukturen daher unterschiedlich umgesetzt werden. In diesem Modul werden diese bisher an konkreten Beispielen behandelten Konzepte systematisch aufbereitet und auf eine breitere Grundlage gestellt, um den Studierenden das notwendige Handwerkszeug für ein systematisches Vorgehen bei der Programmierung zu geben.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Datenstrukturen zu erklären und in konkreten Anwendungsfällen zu vergleichen und anzuwenden.
- grundlegende Algorithmen zu erklären.
- in konkreten Anwendungsfällen geeignete Algorithmen zu entwerfen oder auszuwählen sowie anzuwenden.
- den Einsatz XML als Datenstruktur sowie die wichtigsten Algorithmen und Konzepte zur Verarbeitung von XML-Dokumenten (DOM, SAX, XLS) zu erklären und in einfachen Anwendungsfällen anzuwenden.
- die verbreiteten Programmierparadigmen und Programmiersprachen zu erläutern und zu vergleichen.

## Kursinhalt

1. Grundbegriffe
  - 1.1 Geschichte der Algorithmik
  - 1.2 Detaillierung und Abstraktion
  - 1.3 Kontrollstrukturen
  - 1.4 Datentypen
  - 1.5 Grundlegende Datenstrukturen

2. Datenstrukturen
  - 2.1 Weiterführende Datenstrukturen
  - 2.2 Blockchain
  - 2.3 Abstrakte Datentypen, Objekte und Klassen
3. Algorithmenentwurf
  - 3.1 Induktion, Iteration und Rekursion
  - 3.2 Methoden des Algorithmen-Entwurfs
  - 3.3 Korrektheit und Verifikation von Algorithmen
  - 3.4 Effizienz und Komplexität von Algorithmen
4. Grundlegende Algorithmen
  - 4.1 Traversieren und Linearisieren von Bäumen
  - 4.2 Sortieralgorithmen
  - 4.3 Suche in Zeichenketten
  - 4.4 Hash-Algorithmen
  - 4.5 Mustererkennung
5. XML
  - 5.1 Aufbau von XML-Dokumenten
  - 5.2 Zugriff auf XML-Dokumente mit DOM und SAX
  - 5.3 Transformation von XML-Dokumenten mittels XSL
  - 5.4 JSON als Alternative zu XML
6. Programmiersprachen
  - 6.1 Programmierparadigmen
  - 6.2 Ausführung von Programmen
  - 6.3 Typen von Programmiersprachen
  - 6.4 Syntax, Semantik und Pragmatik
  - 6.5 Variablen und Typsysteme
7. Überblick über wichtige Programmiersprachen
  - 7.1 Die C-Familie
  - 7.2 Java
  - 7.3 Matlab
  - 7.4 COBOL
  - 7.5 PHP und HTML
  - 7.6 Weitere Programmiersprachen

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Gumm H. P. /Sommer M. (2013): Einführung in die Informatik. 10. Auflage. Oldenbourg, München.
- Harel, D. (2006): Algorithmik. Die Kunst des Rechnens. Springer, Berlin/Heidelberg/New York.
- Vonhoegen, H. (2015): Einstieg in XML. Grundlagen, Praxis, Referenz. Rheinwerk Computing, Bonn.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# Theoretische Informatik und Mathematische Logik

Modulcode: DLBITIML

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> DLBIADPS01	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	---	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Robert Graf (Theoretische Informatik und Mathematische Logik)

## Kurse im Modul

- Theoretische Informatik und Mathematische Logik (DLBITIML01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: myStudium

Klausur, 90 Minuten

Studienformat: Fernstudium

Klausur, 90 Minuten

Studienformat: Kombistudium

Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls**

- Aussagen- und Prädikatenlogik
- Endliche Automaten
- Formale Sprachen
- Berechenbarkeit und Turing-Maschinen
- Komplexitätstheorie
- Petri-Netze

**Qualifikationsziele des Moduls****Theoretische Informatik und Mathematische Logik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- aussagenlogische und prädikatenlogische Zusammenhänge zu formulieren und in Programmiersprachen zu übertragen.
- endliche Automaten und reguläre Ausdrücke zur Beschreibung fachlicher Sachverhalte anzuwenden.
- die Chomsky-Hierarchie zu erläutern.
- Grenzen der Beweisbarkeit und der Berechenbarkeit zu benennen.
- die Aussage und die Relevanz des P=NP-Problems zu erläutern.
- Petri-Netze zur Beschreibung fachlicher Sachverhalte anzuwenden.

**Bezüge zu anderen Modulen im Studiengang**

ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung.

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik.

# Theoretische Informatik und Mathematische Logik

Kurscode: DLBITIML01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBIADPS01

## Beschreibung des Kurses

Theoretische Informatik und mathematische Logik beschreiben die theoretischen Grundlagen des Faches Informatik. Dabei handelt es sich aber nicht um „reine Theorie“, sondern diese Grundlagen werden in vielen Teilbereichen der Informatik praktisch angewendet. Dazu gehören beispielsweise die Formulierung von Bedingungen in SQL-Abfragen oder anderen Programmen auf Basis von Aussagen- und Prädikatenlogik, die Nutzung endlicher Automaten zur Spezifikation von Systemen mit Zustandsübergangsdigrammen, und die Modellierung von Geschäft- und anderen Prozessen mit Petri-Netzen. Darüber hinaus analysieren theoretische Informatik und mathematische Logik die Grenzen der Informatik und der Berechenbarkeit, die unabhängig von den verwendeten Technologien und Algorithmen nicht überschritten werden können.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- aussagenlogische und prädikatenlogische Zusammenhänge zu formulieren und in Programmiersprachen zu übertragen.
- endliche Automaten und reguläre Ausdrücke zur Beschreibung fachlicher Sachverhalte anzuwenden.
- die Chomsky-Hierarchie zu erläutern.
- Grenzen der Beweisbarkeit und der Berechenbarkeit zu benennen.
- die Aussage und die Relevanz des P=NP-Problems zu erläutern.
- Petri-Netze zur Beschreibung fachlicher Sachverhalte anzuwenden.

## Kursinhalt

1. Aussagenlogik
  - 1.1 Grundbegriffe
  - 1.2 Aussagenlogische Rechenregeln und Normalformen
  - 1.3 Interpretation und Erfüllbarkeit
  - 1.4 indirekter Beweis und Resolution
  - 1.5 Korrektheit und Vollständigkeit

2. Prädikatenlogik
  - 2.1 Grundbegriffe
  - 2.2 Resolution in der Prädikatenlogik
  - 2.3 Vollständigkeit und Unvollständigkeit
  - 2.4 Logik-Programmierung mit Prolog
3. Endliche Automaten und reguläre Ausdrücke
  - 3.1 Grundbegriffe endlicher Automaten
  - 3.2 Reguläre Ausdrücke und Sprachen
  - 3.3 Praxisanwendungen
4. Formale Sprachen und Grammatiken
  - 4.1 Grundbegriffe
  - 4.2 Die Chomsky-Hierarchie
  - 4.3 Kontextfreie Grammatiken (Typ-2-Grammatiken)
  - 4.4 Kontextsensitive Grammatiken (Typ-1-Grammatiken)
5. Berechenbarkeit und Turing-Maschinen
  - 5.1 Modelle der Berechenbarkeit
  - 5.2 Turing-Maschinen
  - 5.3 Einige weitere Berechnungsmodelle
  - 5.4 Berechenbarkeit, Entscheidbarkeit und das Halteproblem
6. Komplexitätstheorie
  - 6.1 Landau'sche O-Notation
  - 6.2 Grundbegriffe der Komplexitätstheorie
  - 6.3 P=NP?
  - 6.4 NP-vollständige Probleme
7. Petri-Netze
  - 7.1 Grundbegriffe von Graphen und Petri-Netzen
  - 7.2 Modellierung von Eigenschaften nebenläufiger Systeme
  - 7.3 Erreichbarkeit in Petri-Netzen
  - 7.4 Invarianten von Petri-Netzen

- |  |
|--|
| 8. Anwendungen der mathematischen Logik und der theoretischen Informatik |
| 8.1 Compiler   |
| 8.2 Programmkorrektheit  |
| 8.3 Künstliche Intelligenz   |
| 8.4 Kryptologie  |

<b>Literatur</b>
<b>Pflichtliteratur</b>
<b>Weiterführende Literatur</b>
<ul style="list-style-type: none"><li>▪ Dewdney, A.K. (1995): Der Turing Omnibus. Eine Reise durch die Informatik mit 66 Stationen. Springer, Berlin/Heidelberg/New York.</li><li>▪ Erk, K./Priese, L. (2008): Theoretische Informatik. 3. Auflage. Springer eXamen.press, Berlin/Heidelberg.</li><li>▪ Priese, L./Wimmerl, H. (2008): Petri-Netze. 2. Auflage. Springer eXamen.press, Berlin/Heidelberg.</li><li>▪ Schöning, U. (2000): Logik für Informatiker. 5. Auflage. Spektrum Verlag, Heidelberg/ Berlin.</li><li>▪ Schöning, U. (2008): Ideen der Informatik. Grundlegende Modelle und Konzepte der Theoretischen Informatik, 3. Auflage. Oldenbourg, München.</li></ul>

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input checked="" type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input checked="" type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input checked="" type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# IT-Projektmanagement

Modulcode: IPMG-01

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Tobias Brückmann (IT-Projektmanagement)

## Kurse im Modul

- IT-Projektmanagement (IPMG01-01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Fernstudium

Klausur, 90 Minuten

Studienformat: myStudium

Klausur, 90 Minuten

Studienformat: Kombistudium

Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

<p><b>Lehrinhalt des Moduls</b></p> <ul style="list-style-type: none"> <li>▪ Begriffe und Grundlagen im IT-Projektmanagement</li> <li>▪ Planungstechniken im Großen und Kleinen</li> <li>▪ Techniken zu Priorisierung, Aufwandschätzung, Projektcontrolling</li> <li>▪ Techniken zu Stakeholder-, Kommunikations- und Risikomanagement</li> <li>▪ Organisation und Struktur von IT-Projekten</li> <li>▪ PITPM - Pragmatisches IT- Projektmanagement</li> </ul>	
<p><b>Qualifikationsziele des Moduls</b></p> <p><b>IT-Projektmanagement</b></p> <p>Nach erfolgreichem Abschluss sind die Studierenden in der Lage,</p> <ul style="list-style-type: none"> <li>▪ Grundprinzipien und Aufgaben von IT-Projektmanagement zu erläutern und voneinanderabzugrenzen.</li> <li>▪ Techniken zur Planung und zur operativen Steuerung von IT-Projekten zu erläutern und voneinander abzugrenzen.</li> <li>▪ ausgewählte Techniken und Methoden zum Stakeholder-, Kommunikations- und Risikomanagement zu beschreiben.</li> <li>▪ Organisation und Struktur von IT-Projekten anhand ausgewählter Managementmodelle zu erläutern.</li> <li>▪ Aktivitäten zur Konfiguration und Steuerung von IT-Projekten nach PITPM kennen und beschreiben können.</li> </ul>	
<p><b>Bezüge zu anderen Modulen im Studiengang</b></p> <p>Ist Grundlage für weitere Module im Bereich Informatik &amp; Software-Entwicklung</p>	<p><b>Bezüge zu anderen Studiengängen der Hochschule</b></p> <p>Alle Bachelor-Programme im Bereich IT &amp; Technik</p>

# IT-Projektmanagement

Kurscode: IPMG01-01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

In diesem Kurs werden typische Probleme beim Management von SW-Projekten diskutiert und dabei Methoden und Techniken vermittelt, mit denen die Herausforderungen gezielt adressiert werden können. Darüber hinaus werden Standard-Vorgehensmodelle für das IT-Projektmanagement erläutert und gezielt deren Stärken und Schwächen herausgearbeitet.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundprinzipien und Aufgaben von IT-Projektmanagement zu erläutern und voneinander abzugrenzen.
- Techniken zur Planung und zur operativen Steuerung von IT-Projekten zu erläutern und voneinander abzugrenzen.
- ausgewählte Techniken und Methoden zum Stakeholder-, Kommunikations- und Risikomanagement zu beschreiben.
- Organisation und Struktur von IT-Projekten anhand ausgewählter Managementmodelle zu erläutern.
- Aktivitäten zur Konfiguration und Steuerung von IT-Projekten nach PITPM kennen und beschreiben können.

## Kursinhalt

1. Begriffe und Grundlagen im IT-Projektmanagement
  - 1.1 Projektbegriff und Arten von IT-Projekten
  - 1.2 IT-Projektlebenszyklus
  - 1.3 Multiprojektmanagement – Das Projekt im Kontext der Organisation
2. Planungstechniken
  - 2.1 Planung im Großen: Meilensteine, Teilaufgaben, Arbeitspakete
  - 2.2 Planung im Großen: Gantt-Diagramme
  - 2.3 Operative Planung und Organisation: Kanban Boards, Backlog

3. Priorisierung, Aufwandschätzung, Projektcontrolling
  - 3.1 Priorisierung
  - 3.2 Aufwandsschätzung
  - 3.3 Projektcontrolling
4. Stakeholder-, Kommunikations- und Risikomanagement
  - 4.1 Stakeholder Management
  - 4.2 Kommunikationsmanagement
  - 4.3 Risikomanagement
5. Organisation und Struktur von IT-Projekten
  - 5.1 Ausgewählte Managementmodelle: Scrum, PITPM, PRINCE2
  - 5.2 PRINCE2 - Überblick und ausgewählte Prozesse
  - 5.3 SCRUM – Überblick, Rollen, Artefakte
6. PITPM - Pragmatisches IT-Projektmanagement
  - 6.1 Struktur und Phasen in PITPM
  - 6.2 IT-Projekt konfigurieren
  - 6.3 IT-Projekt steuern

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Gabler Wirtschaftslexikon (2019). Stichwort. Projekt. Springer Gabler.
- Kuster, J. et al (2019). Handbuch Projektmanagement. 3. Auflage, Springer.
- Wieczorrek, H. W. & Mertens, P. (2011). Management von IT-Projekten. 4. Auflage, Springer.
- Rook, A. (2011). Software-Kanban – eine Einführung. In: Projektmagazin, Heft 4.
- Schwaber, K. & Sutherland, J. (2020). The Scrum Guide.
- Hummel, O. (2011). Aufwandsschätzungen in der Software- und Systementwicklung kompakt.Spektrum.
- Spitzcok von Brisinski N., Vollmer G., Weber-Schäfer U. (2014). Pragmatisches IT-Projektmanagement (PITPM). 2. Auflage, dpunkt.
- Stelzer, D. & Bratfisch, W. (2006). Earned-Value-Analyse – ein Verfahren zur Fortschrittskontrolle und -prognose von IT-Projekten. Ilmenauer Beiträge zur Wirtschaftsinformatik, Heft 10.
- Bentley, C. (2019). Concise PRINCE2® - Principles and Essential Themes (3rd Edition). IT Governance Publishing.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

IPMG01-01

## DevSecOps und gängige Software-Schwachstellen

Modulcode: DLBCSEDCSW\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> DLBCSESPB01_D oder DLBCSESPB01_E	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof. Dr. Stephan Spitz (DevSecOps und gängige Software-Schwachstellen)

### Kurse im Modul

- DevSecOps und gängige Software-Schwachstellen (DLBCSEDCSW01\_D)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Schriftliche Ausarbeitung: Hausarbeit

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

- Häufige Code-Fehler
- Software-Entwicklungs-Lebenszyklus
- DevOps
- DevSecOps
- Schwachstellenberichte und Bug-Bounty-Programme
- Patch-Steuerung

**Qualifikationsziele des Moduls****DevSecOps und gängige Software-Schwachstellen**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- häufige Software-Implementierungs- und Entwurfsfehler zu vermeiden.
- einen Softwareentwicklungs-Lebenszyklusprozess auf der Grundlage der DevSecOps-Prinzipien zu entwerfen.
- Schwachstellenberichte und -reaktionen in die SDL aufzunehmen.
- ein Bug-Bounty-Programm zu organisieren und zu steuern.
- einen unternehmensweiten Patch-Management-Prozess zu implementieren und zu steuern.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# DevSecOps und gängige Software-Schwachstellen

Kurscode: DLBCSEDCSW01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSESPB01_D oder DLBCSESPB01_E

## Beschreibung des Kurses

Moderne Organisationen sind bis zu einem gewissen Grad von Software abhängig. In vielen Fällen ist es die kundenspezifische Software in Geschäftsprozessen oder Produkten, die das Hauptunterscheidungsmerkmal darstellt. Aber auch Unternehmen, die keine eigene Entwicklung betreiben, sind auf Software angewiesen, und das Verständnis von Software-Schwachstellen ist für ihren Betrieb lebenswichtig, wie die jüngsten Ransomware-Angriffe gezeigt haben. In diesem Kurs beschäftigen wir uns mit moderner Software-Entwicklung und Lebenszyklus-Prozessen. Seit den Anfängen mit Extremer Programmierung hat es eine Verlagerung weg vom linearen Wasserfallmodell hin zu einem agilen Entwicklungsprozess gegeben. In jüngerer Zeit hat sich die „Shift-Left“-Entwicklung dafür eingesetzt, dass Sicherheit von Anfang an und nicht erst im Nachhinein berücksichtigt wird. Um sichere Software zu entwerfen, ist es natürlich wichtig zu verstehen, wie sich Schwachstellen in den Code einschleichen. Wir sehen uns die wichtigsten Aufzählungen von Softwarefehlern an: OWASP und die CWEs von Mitre. Schließlich ist das Patch-Management zum wichtigsten Abwehrinstrument für eine Organisation geworden. Wir betrachten dieses Thema sowohl aus der Perspektive der Softwareentwicklung als auch aus der Sicht des Kunden.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- häufige Software-Implementierungs- und Entwurfsfehler zu vermeiden.
- einen Softwareentwicklungs-Lebenszyklusprozess auf der Grundlage der DevSecOps-Prinzipien zu entwerfen.
- Schwachstellenberichte und -reaktionen in die SDL aufzunehmen.
- ein Bug-Bounty-Programm zu organisieren und zu steuern.
- einen unternehmensweiten Patch-Management-Prozess zu implementieren und zu steuern.

### Kursinhalt

1. Einführung in den Software-Entwicklungsprozess
  - 1.1 Traditionelle Software-Entwicklung: Wasserfall-Methodik
  - 1.2 Iterativer Entwurf
  - 1.3 Agile Software-Entwicklung
  - 1.4 Operationen als separater Prozess
  - 1.5 Infrastruktur als Code
  - 1.6 Zusammenlegung von Entwicklung und Betrieb: DevOps
2. Bewährte Praktiken von DevOps
  - 2.1 Codierung: Code-Entwicklung und -Überprüfung, Quellcode-Verwaltungstools, Code-Zusammenführung.
  - 2.2 Build: kontinuierliche Integrationswerkzeuge, Build-Status.
  - 2.3 Tests: Instrumente für kontinuierliche Tests, die ein schnelles und zeitnahes Feedback zu Geschäftsrisiken liefern.
  - 2.4 Paketierung: Artefakt-Repository, Staging vor der Bereitstellung der Anwendung.
  - 2.5 Freigabe: Änderungsmanagement, Freigabegenehmigungen, Freigabeautomatisierung.
  - 2.6 Konfigurieren: Konfiguration und Verwaltung der Infrastruktur, Infrastruktur als Code-Tools.
  - 2.7 Überwachung: Überwachung der Anwendungsleistung, Endbenutzer-Erfahrung.
3. Quellen von Sicherheitsfehlern
  - 3.1 Allgemeine Klassen von Fehlern
  - 3.2 Ein Blick auf die OWASP-Top Ten
  - 3.3 Blick auf die Mitra CWE™
4. DevSecOps
  - 4.1 Schutzziele
  - 4.2 Modellierung von Bedrohungen
  - 4.3 Wahl der Programmiersprache, Werkzeugkette und Infrastruktur
  - 4.4 Linting bei Fragen der Codesicherheit
  - 4.5 Prüfung auf Sicherheit
  - 4.6 Sicherheit durch Design/Shifting Left
  - 4.7 Der Mensch als ein Problem der Sicherheit
  - 4.8 Entwerfen in einem Fehlerbericht- und Antwortprozess
  - 4.9 Steuern eines Bug-Bounty-Programms

5. Patch-Verwaltung
  - 5.1 Dilemma: Auslassen von Software-Update- vs. Sicherheit
  - 5.2 Offenlegung von Schwachstellen und der Mitre CVE™ Prozess
  - 5.3 Koordinierte Offenlegung von Schwachstellen
  - 5.4 Programmsicherheit vs. Software-as-a-Service-Patching
  - 5.5 Einsatzstrategien für das frühzeitige Abfangen von Bugs
6. Zusammenfassung und Forschungsprobleme

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Anderson, R. (2020): Security Engineering. 3rd edition, Wiley, Hoboken, NJ.
- Mitre CVEs: <https://cwe.mitre.org>
- OWASP Top-ten: <https://owasp.org/www-project-top-ten/>

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Hausarbeit

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien







# 4. Semester

---



# IT-Service-Management

Modulcode: IWSM1

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. André Köhler (IT-Service-Management )

## Kurse im Modul

- IT-Service-Management (IWSM01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Fernstudium  
Klausur oder Advanced Workbook, 90 Minuten

Studienformat: Kombistudium  
Klausur oder Advanced Workbook, 90 Minuten

Studienformat: myStudium  
Klausur oder Advanced Workbook, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

<p><b>Lehrinhalt des Moduls</b></p> <ul style="list-style-type: none"> <li>▪ Grundlagen und Begriffe zum IT-Servicemanagement</li> <li>▪ ITIL - Service Lifecycle, Service Strategy und Continual Service Improvement</li> <li>▪ ITIL – Service Design</li> <li>▪ ITIL – Service Transition</li> <li>▪ ITIL – Service Operation</li> <li>▪ Information Security Management mit dem IT-Grundschutz-Framework des BSI</li> </ul>	
<p><b>Qualifikationsziele des Moduls</b></p> <p><b>IT-Servicemanagement</b></p> <p>Nach erfolgreichem Abschluss sind die Studierenden in der Lage,</p> <ul style="list-style-type: none"> <li>▪ die Grundlagen und Herausforderungen des IT-Servicemanagements zu benennen.</li> <li>▪ die Motivation und den Aufbau der IT Infrastructure Library (ITIL) zu beschreiben, die Hauptelemente zu bestimmen und konkrete Aktivitäten im Service Lifecycle zu unterscheiden.</li> <li>▪ die Aktivitäten der ITIL-Governance und ITIL-Operational-Prozesse darzustellen, einander gegenüberzustellen und konkrete Lösungen unter Anwendung der Aktivitäten zu erarbeiten.</li> </ul>	
<p><b>Bezüge zu anderen Modulen im Studiengang</b></p> <p>Ist Grundlage für alle weiteren Module aus dem Bereich Informatik &amp; Software-Entwicklung</p>	<p><b>Bezüge zu anderen Studiengängen der Hochschule</b></p> <p>Alle Bachelor-Programme aus dem Bereich IT &amp; Technik</p>

# IT-Service-Management

Kurscode: IWSM01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

IT-Service-Management ist ein Ansatz, die IT eines Unternehmens als Dienstleister und Unterstützer der betrieblichen und geschäftlichen Prozesse auszurichten und zu verstehen. Hierbei stehen Qualitätsmanagement und Handhabung des täglichen Betriebs im Vordergrund. Dieser Kurs vermittelt unter Verwendung der IT Infrastructure Library (ITIL) Konzepte, Vorgehensweisen und Best Practices im Bereich IT-Service-Management (IT-Betrieb). Damit werden also die Steuerung der Aktivitäten eines SW-Lebenszyklus betrachtet, die nach der Entwicklung eines IT-Systems stattfinden: der IT-Betrieb als kontinuierlichen Lauf des produktiven Tagesgeschäfts der IT-Abteilungen eines Unternehmens.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen und Herausforderungen des IT-Service-Managements zu benennen.
- die Motivation und den Aufbau der IT Infrastructure Library (ITIL) zu beschreiben, die Hauptelemente zu bestimmen und konkrete Aktivitäten im Service Lifecycle zu unterscheiden.
- die Aktivitäten der ITIL-Governance und ITIL-Operational-Prozesse darzustellen, einander gegenüberzustellen und konkrete Lösungen unter Anwendung der Aktivitäten zu erarbeiten.

## Kursinhalt

1. Grundlagen und Begriffe zum IT-Service Management
  - 1.1 IT-Dienstleistungen
  - 1.2 IT-Service-Management
2. ITIL - Service Lifecycle, Service Strategy und Continual Service Improvement
  - 2.1 Service Lifecycle
  - 2.2 Service Strategy
  - 2.3 Continual Service Improvement

3. ITIL – Service Design
  - 3.1 Service Level Management
  - 3.2 Service Catalog Management
  - 3.3 Availability Management
  - 3.4 Weitere Prozesse im Service Design
4. ITIL – Service Transition
  - 4.1 Transition Planning and Support
  - 4.2 Change Management
  - 4.3 Service Asset and Configuration Management
  - 4.4 Weitere Prozesse in der Service Transition
5. ITIL – Service Operation
  - 5.1 Incident Management
  - 5.2 Problem Management
  - 5.3 Weitere Prozesse in der Service Operation
6. Information Security Management mit dem IT-Grundschutz Framework des BSI
  - 6.1 Aufbau und Elemente des BSI-Grundschutzes
  - 6.2 Informationssicherheitsprozess

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Beims, M. (2012): IT-Service Management in der Praxis mit ITIL. 3. Auflage, Carl Hanser, München.
- Böttcher, R. (2013): IT-Service Management mit ITIL – 2011 Edition. Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen. Heise, dpunkt, Heidelberg.
- Bundesamt für Sicherheit in der Informationstechnik (2008a): BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise. (Im Internet verfügbar).
- Bundesamt für Sicherheit in der Informationstechnik (2008b): BSI-Standard 100-1. Managementsystem für Informationssicherheit (ISMS). (Im Internet verfügbar).
- Bundesamt für Sicherheit in der Informationstechnik (2014): IT-Grundschutz-Kataloge. 14. Ergänzungslieferung. (Im Internet verfügbar).
- Kleiner, F. (2013): IT Service Management. Aus der Praxis für die Praxis. Springer Vieweg, Heidelberg.
- Scholderer, R. (2011): Management von Service-Level-Agreements. Methodische Grundlagen und Praxislösungen mit COBIT, ISO 20000 und ITIL. 2. Auflage, dpunkt, Heidelberg.



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Advanced Workbook, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
100 h	0 h	25 h	25 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Advanced Workbook, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
100 h	0 h	25 h	25 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Advanced Workbook, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
100 h	0 h	25 h	25 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

IWSM01

# Kryptografische Verfahren

Modulcode: DLBISIC2-01

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Ralf Kneuper (Kryptografische Verfahren)

## Kurse im Modul

- Kryptografische Verfahren (DLBISIC02-01)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Fernstudium  
Schriftliche Ausarbeitung: Fallstudie

Studienformat: Kombistudium  
Schriftliche Ausarbeitung: Fallstudie

Studienformat: myStudium  
Schriftliche Ausarbeitung: Fallstudie

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

<p><b>Lehrinhalt des Moduls</b></p> <ul style="list-style-type: none"> <li>▪ Schutzziele, Schwachstellen und Bedrohungen</li> <li>▪ Kryptologische Grundlagen und kryptografische Bausteine</li> <li>▪ Kryptografische Grundanwendungen</li> <li>▪ Authentifikation</li> <li>▪ Sicherung von Einzelrechnern</li> <li>▪ Sicherheit in Kommunikationsnetzen</li> <li>▪ Sicherheit im E-Commerce</li> <li>▪ Sichere Softwareentwicklung</li> </ul>	
<p><b>Qualifikationsziele des Moduls</b></p> <p><b>Kryptografische Verfahren</b></p> <p>Nach erfolgreichem Abschluss sind die Studierenden in der Lage,</p> <ul style="list-style-type: none"> <li>▪ Überblickswissen über verschiedene Klassen kryptografischer Systeme wiederzugeben.</li> <li>▪ symmetrische kryptographische Verfahren, insbesondere One-Time Pad, DES, AES, zu erläutern und deren Funktionsweise anhand konkreter, einfacher Beispiele zu beschreiben.</li> <li>▪ Hashfunktionen zu erklären.</li> <li>▪ asymmetrische kryptographische Verfahren, insbesondere RSA, zu erläutern und deren Funktionsweise anhand konkreter, einfacher Beispiele zu beschreiben.</li> <li>▪ Einsatzbereiche und Anwendungsszenarien für kryptografische Verfahren zu skizzieren.</li> </ul>	
<p><b>Bezüge zu anderen Modulen im Studiengang</b></p> <p>Ist Grundlage für alle weiteren Module aus dem Bereich Informatik &amp; Software-Entwicklung</p>	<p><b>Bezüge zu anderen Studiengängen der Hochschule</b></p> <p>Alle Bachelor-Programme im Bereich IT &amp; Technik</p>

# Kryptografische Verfahren

Kurscode: DLBISIC02-01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Dieser Kurs vermittelt Basiswissen und gezieltes Vertiefungswissen zu kryptographischen Verfahren und dem praktischen Einsatz kryptografischer Systeme. Nach einem Überblick über kryptographische Verfahren werden sowohl Hashfunktionen als auch symmetrische Verfahren und asymmetrische Verfahren vorgestellt. Dabei werden zu ausgewählten Verfahren die theoretischen Grundlagen vermittelt und anhand einfacher Beispiele praktisch nachvollzogen. Darüber hinaus werden Einsatzbereiche und Anwendungsszenarien für kryptografische Verfahren vorgestellt.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Überblickswissen über verschiedene Klassen kryptografischer Systeme wiederzugeben.
- symmetrische kryptographische Verfahren, insbesondere One-Time Pad, DES, AES, zu erläutern und deren Funktionsweise anhand konkreter, einfacher Beispiele zu beschreiben.
- Hashfunktionen zu erklären.
- asymmetrische kryptographische Verfahren, insbesondere RSA, zu erläutern und deren Funktionsweise anhand konkreter, einfacher Beispiele zu beschreiben.
- Einsatzbereiche und Anwendungsszenarien für kryptografische Verfahren zu skizzieren.

## Kursinhalt

1. Schutzziele, Schwachstellen und Bedrohungen
  - 1.1 Schutzziele
  - 1.2 Schwachstellen und Bedrohungen
2. Kryptologische Grundlagen und kryptografische Bausteine
  - 2.1 Verschlüsselung
  - 2.2 Symmetrische Verschlüsselung
  - 2.3 Asymmetrische Verschlüsselung
  - 2.4 Einwegfunktionen und kryptografische Hashfunktionen

3. Kryptografische Grundanwendungen
  - 3.1 Schlüsselaustausch und hybriden Verfahren
  - 3.2 Digitale Unterschrift
  - 3.3 Message Authentication Code
  - 3.4 Steganografische Verfahren
4. Authentifikation
  - 4.1 Passwörter und Public-Key-Zertifikate
  - 4.2 Challenge-Response-Verfahren und Zero-Knowledge-Verfahren
  - 4.3 Biometrische Verfahren
  - 4.4 Authentifikation in verteilten Systemen
  - 4.5 Identitäten durch Smartcards
5. Sicherung von Einzelrechnern
  - 5.1 Schadsoftware und Cookies
  - 5.2 Einige Besonderheiten bei Betriebssystemen
  - 5.3 Sicherheit von Webservern
6. Sicherheit in Kommunikationsnetzen
  - 6.1 Sicherheitsprobleme und Abwehrkonzepte
  - 6.2 Internet-Standards für die Kommunikationssicherheit
  - 6.3 Identität und Anonymität
  - 6.4 Sicherheit in der mobilen und der drahtlosen Kommunikation
7. Sicherheit im E-Commerce
  - 7.1 E-Mail-Sicherheit
  - 7.2 Online-Banking und Onlinebezahlen
  - 7.3 Elektronisches Geld
8. Sichere Softwareentwicklung
  - 8.1 Bedrohungsmodellierung
  - 8.2 Sicherer Softwareentwurf
  - 8.3 Techniken für sicheres Programmieren



**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Eckert, C. (2014): IT-Sicherheit. Konzepte – Verfahren – Protokolle. 9. Auflage, Oldenbourg Wissenschaftsverlag, München.
- Ertel, W. (2012): Angewandte Kryptographie. Carl Hanser, München.
- Heiderich, M. et al. (2009): Sichere Webanwendungen. Galileo Press, Bonn.
- Paulus, S. (2011): Basiswissen sichere Software. dpunkt, Heidelberg.
- Poguntke, W. (2013): Basiswissen IT-Sicherheit. 3. Auflage, W3L-AG, Dortmund.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

## IT-Recht

Modulcode: DLBIITR

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof. Dr. Andreas Walter (IT-Recht)

### Kurse im Modul

- IT-Recht (DLBIITR01)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium

Klausur, 90 Minuten

Studienformat: Kombistudium

Klausur, 90 Minuten

Studienformat: Duales Studium

Klausur, 90 Minuten

Studienformat: myStudium

Klausur, 90 Minuten

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

<p><b>Lehrinhalt des Moduls</b></p> <ul style="list-style-type: none"> <li>▪ IT-Recht und seine Einbettung in das Rechtssystem</li> <li>▪ Vertragstypen</li> <li>▪ Softwarelizenzmodelle</li> <li>▪ Schutz- und Informationsrechte</li> <li>▪ Internetrecht und Telekommunikationsrecht</li> <li>▪ Datenschutz</li> </ul>	
<p><b>Qualifikationsziele des Moduls</b></p> <p><b>IT-Recht</b></p> <p>Nach erfolgreichem Abschluss sind die Studierenden in der Lage,</p> <ul style="list-style-type: none"> <li>▪ die wesentlichen nationalne und internationalen Rechtsgrundlagen und Rahmenbedingungen des IT-Rechts zu erinnern.</li> <li>▪ die rechtlichen Grundlagen zum Datenschutzrecht auf einfache Anwendungsfälle anzuwenden.</li> <li>▪ in Anwendungsfällen die geeignete Vertragsform oder das geeignete Lizenzmodell auszuwählen und die Auswirkungen dieser Auswahl zu erläutern.</li> <li>▪ die verschiedenen Schutz- und Informationsrechte zu erläutern.</li> <li>▪ die rechtlichen Grundlagen zum Internet- und Telekommunikationsrecht zu erläutern.</li> <li>▪ komplexe rechtliche Fragestellungen zu erkennen, die spezialisiertes juristisches Knowhow erfordern, und rechtliche Stellungnahmen im eigenen Kontext zu interpretieren.</li> </ul>	
<p><b>Bezüge zu anderen Modulen im Studiengang</b></p> <p>Ist Grundlage für weitere Module im Bereich Recht</p>	<p><b>Bezüge zu anderen Studiengängen der Hochschule</b></p> <p>Alle Bachelor-Programme im Bereich Wirtschaft &amp; Management</p>

# IT-Recht

Kurscode: DLBIITR01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Die Informatik ist in einen rechtlichen Rahmen eingebettet, der bei der Arbeit zu berücksichtigen ist. Dies betrifft einerseits die eigene Gestaltung dieser Arbeit, die beispielsweise durch Verträge und das zugehörige Vertragsrecht bestimmt wird. Andererseits gestaltet die Informatik auch stark ihr Umfeld und muss dabei relevante rechtliche Grundlagen wie das Telekommunikationsrecht oder das Datenschutzrecht berücksichtigen. Ziel dieses Kurses ist es daher, die Studierenden in die Lage zu versetzen, die speziellen IT-Aspekte in diesem rechtlichen Rahmen zu berücksichtigen, in einfachen Fällen anzuwenden, und zu erkennen, wenn spezialisiertes juristisches Knowhow erforderlich wird.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wesentlichen nationalne und internationalen Rechtsgrundlagen und Rahmenbedingungen des IT-Rechts zu erinnern.
- die rechtlichen Grundlagen zum Datenschutzrecht auf einfache Anwendungsfälle anzuwenden.
- in Anwendungsfällen die geeignete Vertragsform oder das geeignete Lizenzmodell auszuwählen und die Auswirkungen dieser Auswahl zu erläutern.
- die verschiedenen Schutz- und Informationsrechte zu erläutern.
- die rechtlichen Grundlagen zum Internet- und Telekommunikationsrecht zu erläutern.
- komplexe rechtliche Fragestellungen zu erkennen, die spezialisiertes juristisches Knowhow erfordern, und rechtliche Stellungnahmen im eigenen Kontext zu interpretieren.

## Kursinhalt

1. Einführung in die Grundlagen des Rechts und IT-Rechts
  - 1.1 Aufbau des deutschen Rechtssystems
  - 1.2 Bürgerliches Recht
  - 1.3 Handelsrecht
  - 1.4 Übersicht über das Rechtsgebiet IT-Recht
  - 1.5 Internationale Rahmenbedingungen des IT-Rechtes
  - 1.6 IT-spezifisches Strafrecht

2. Typische Vertragstypen in der IT
  - 2.1 Hardware-Verträge
  - 2.2 Softwareüberlassung
  - 2.3 Projektverträge
  - 2.4 Besonderheiten bei agiler Vorgehensweise
  - 2.5 Beratungs- und Wartungsverträge
  - 2.6 Cloud Computing, Outsourcing und Hosting
  - 2.7 Besonderheiten bei der öffentlichen Vergabe von IT-Leistungen
  - 2.8 Kartellrecht
3. Softwarelizenzmodelle
  - 3.1 Lizenzen und Softwareüberlassung
  - 3.2 Standardklauseln
  - 3.3 Durchsetzung von Lizenzen durch Digital Rights Management (DRM)
  - 3.4 Open Source Software, Free- und Shareware
4. Schutz- und Informationsrechte
  - 4.1 Patent- und Markenrecht
  - 4.2 Urheberrecht
  - 4.3 Schutzfähigkeit von Software
  - 4.4 Abmahnungen
  - 4.5 Informationsfreiheitsgesetz
5. Internet- und Telekommunikationsrecht
  - 5.1 Telekommunikationsgesetz
  - 5.2 Telemediengesetz
  - 5.3 Verantwortung für Inhalte im Internet
  - 5.4 Domainrecht
  - 5.5 Elektronische Signaturen
  - 5.6 Elektronische Vertragsschließung
  - 5.7 Elektronischer Geschäftsverkehr und Onlineshopping



6. Datenschutz und IT-Sicherheit
  - 6.1 Grundlagen des Datenschutzes
  - 6.2 EUDSGVO, DSAnpUG-EU und BDSG(-Neu)
  - 6.3 Datenschutz-Anforderungen an Organisationen
  - 6.4 Datenschutzrechte der betroffenen Person
  - 6.5 Datenschutz bei Datenübermittlung in Drittländer
  - 6.6 IT-Sicherheit und Gesetze
  - 6.7 Funktionale Sicherheit und Produkthaftung

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Auer-Reinsdorff, A./Conrad, I. (2011): Beck'sches Mandatshandbuch IT-Recht. C.H.Beck Verlag, München.
- Hoeren, T. (2017): IT-Recht. Skriptum. (<https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien>[letzter Zugriff 20.03.2018]).
- Sodtalbers, A./Volmann, A./Heise, A. (2010): IT-Recht. W3L Verlag, Witten-Herdecke.
- Voigt, P./von dem Bussche, A. (2018): EU-Datenschutz-Grundverordnung (DSGVO). Praktikerhandbuch. Springer, Berlin.
- Zahrnt, C. (2014): IT-Projektverträge. Rechtlich richtig vorgehen. CreateSpace Independent Publishing Platform.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

**Studienformat Duales Studium**

<b>Studienform</b> Duales Studium	<b>Kursart</b> Integrierte Vorlesung
--------------------------------------	---

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
129,75 h	13,5 h	6,75 h	0 h	0 h	150 h

<b>Lehrmethoden</b>
Der Kurs verbindet die interaktive Präsenzlehre mit einer online unterstützten Selbstlernphase. Während der Präsenzphase werden Studierende gezielt bei der Übung und Vertiefung der vermittelten Inhalte begleitet.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBIITR01

## Host- und Softwareforensik

Modulcode: DLBCSEHSF\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> DLBCSESPB01_D oder DLBCSESPB01_E	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Dr. Andreas Schmidt (Host- und Softwareforensik)

### Kurse im Modul

- Host- und Softwareforensik (DLBCSEHSF01\_D)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Klausur, 90 Minuten

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

- Werkzeuge und Methoden für die Host-Forensik
- Schadsoftware-Sandboxing und Reverse Engineering
- Verfassen von Berichten und Präsentationen

**Qualifikationsziele des Moduls****Host- und Softwareforensik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Anforderungen an die system-forensische Analyse zu verstehen.
- die verfügbaren Tools und Methoden zur Sammlung und Analyse von Hinweisen zu kennen.
- die Prinzipien des Malware-Sandboxing und Reversierung zu verstehen.
- Berichte und Präsentationen unter Berücksichtigung des Zielpublikums zu verfassen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung.

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik.



# Host- und Softwareforensik

Kurscode: DLBCSEHSF01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSESPB01_D oder DLBCSESPB01_E

## Beschreibung des Kurses

Sicherheitsbeauftragte werden heutzutage regelmäßig mit Sicherheitsvorfällen konfrontiert und werden aufgefordert, Schäden zu untersuchen. In diesem Kurs werden sowohl kriminelle Vorfälle als auch Verletzungen der geschäftspolitischen Vorgaben untersucht. Insbesondere geht es darum, wie man Beweise sammelt und auswertet. Wir untersuchen verschiedene Arten unerwünschter Aktivitäten und wie sich diese in den von uns gesammelten Daten manifestieren. Mit den entsprechenden Werkzeugen können Hinweise gesammelt und gegebenenfalls eine Beweismittelkette mit geeigneten kryptographischen Methoden sichergestellt werden. Das Erfassen der Dateien auf einem Datenträger ist gängige Praxis in der Computerforensik. Ein Teil des Beweiserhebungsprozesses ist jedoch auch die Erfassung von Informationen aus dem laufenden System, wozu auch die Speicher- und Prozesserfassung gehört. Die gesammelten Hinweise müssen angemessen ausgewertet und logische Schlussfolgerungen daraus gezogen werden. Häufig wird mögliche Schadsoftware auf dem Opfersystem gefunden. Wir betrachten zwei Methoden zur Analyse der Schadsoftware: Sandboxing und Reverse Engineering. Die Ergebnisse werden in einem Bericht festgehalten, wobei zu berücksichtigen ist, wer das Zielpublikum des Berichts und der möglichen Präsentation sein wird. Gute Kommunikation ist hier von entscheidender Bedeutung.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Anforderungen an die system-forensische Analyse zu verstehen.
- die verfügbaren Tools und Methoden zur Sammlung und Analyse von Hinweisen zu kennen.
- die Prinzipien des Malware-Sandboxing und Reversierung zu verstehen.
- Berichte und Präsentationen unter Berücksichtigung des Zielpublikums zu verfassen.

## Kursinhalt

1. Prinzipien der Computer-Forensik
  - 1.1 Grundlagen der Untersuchung: Kriminalität vs. Geschäftspolitik
  - 1.2 Richtlinien, rechtliche Rahmenbedingungen und Standards
  - 1.3 Sachverständige Zeugen

2. Digitale Beweise
  - 2.1 Arten von Beweisen
  - 2.2 Überlegungen zur Erhebung und zur Beweissicherungskette
  - 2.3 Identifikation
  - 2.4 Auswertung
  - 2.5 Präsentation
3. Zusammenstellung der Beweise aus den Systemen
  - 3.1 Software-Tools und Hardware-Unterstützung
  - 3.2 Kryptographische Methoden zur Sicherstellung der Integrität und Beweissicherungskette
  - 3.3 Schritte der Tatortsuche
  - 3.4 Cloud und mobile Endgeräte
  - 3.5 Festplatten und SSD
4. Computerforensik
  - 4.1 Speicheranalyse
  - 4.2 Auszug und Analyse der Prozesse
  - 4.3 Forensik auf der Ebene der Betriebssysteme
  - 4.4 Forensik in Cloud-Umgebungen
5. Malware Sandboxing
  - 5.1 Kommerzielle und Open-Source-Tools
  - 5.2 Betrachtungen im Gastsystem
  - 5.3 Ausführung von inaktiver, langsamer oder verzögerter Malware
  - 5.4 Interpretation von Berichten der Sandbox
6. Prinzipien des Reverse Engineering
  - 6.1 Reinraum-Design
  - 6.2 Prinzipien von Disassembly
  - 6.3 Maschinencode
  - 6.4 Dekompilierung
7. Auswertung
  - 7.1 Zusammenhänge herstellen
  - 7.2 Ursachenanalyse
  - 7.3 Mapping auf Mitre ATT&CK® Techniques, Tactics and Procedures
  - 7.4 Vermeidung vorschneller Schlüsse

## 8. Präsentation

- 8.1 Verfassen des Berichts
- 8.2 Zusammenarbeit bei der Durchsetzung von Gesetzen
- 8.3 Vorbereitung für die Präsentation vor Gericht
- 8.4 Vorbereitung für die Präsentation beim Management

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Dewald, A. (2015). Forensische Informatik. Deutschland: BoD - Books on Demand.
- Geschonneck, A.(2014).Computer-Forensik (iX Edition): Computerstraftaten erkennen, ermitteln, aufklären. Deutschland:dpunkt.verlag.
- Meseke, B. (2019). Digitale Forensik: Praxiswissen Cybercrime für Manager. Deutschland: Erich Schmidt Verlag GmbH & Company.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- Reddy, N. (2019): Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations. Apress.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: <https://beginners.re/> (last accessed: 24 August 2020)

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

# Artificial Intelligence

Modulcode: DLBDSEAIS1\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Kristina Schaaff (Artificial Intelligence)

## Kurse im Modul

- Artificial Intelligence (DLBDSEAIS01\_D)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Fernstudium  
Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

## Lehrinhalt des Moduls

- Geschichte der KI
- Moderne KI-Systeme
- Bestärkendes Lernen
- Verarbeitung natürlicher Sprache
- Computer Vision

**Qualifikationsziele des Moduls****Artificial Intelligence**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die historische Entwicklung der künstlichen Intelligenz zu erläutern.
- den Ansatz aktueller KI-Systeme zu verstehen.
- die Konzepte hinter dem bestärkenden Lernen zu verstehen.
- natürliche Sprache mit grundlegenden NLP-Techniken zu analysieren.
- Bilder und ihre Inhalte zu untersuchen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Data Science & Artificial Intelligence

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Artificial Intelligence

Kurscode: DLBDSEAIS01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Die Suche nach künstlicher Intelligenz (KI) hat das Interesse der Menschheit seit vielen Jahrzehnten begeistert und ist seit den 1960er Jahren ein aktives Forschungsgebiet. Dieser Kurs gibt einen detaillierten Überblick über die historischen Entwicklungen, Erfolge und Rückschläge der KI sowie über moderne Ansätze in der Entwicklung der künstlichen Intelligenz. Dieser Kurs gibt eine Einführung in das bestärkende Lernen, einem Prozess, der dem ähnelt, wie Menschen und Tiere die Welt erleben: die Umwelt zu erforschen und die beste Vorgehensweise abzuleiten. In diesem Kurs werden auch die Prinzipien der natürlichen Sprachverarbeitung und der Computer Vision (computerbasiertes Sehen) behandelt, beides Schlüsselkomponenten für eine künstliche Intelligenz, die in der Lage ist, mit ihrer Umgebung zu interagieren.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die historische Entwicklung der künstlichen Intelligenz zu erläutern.
- den Ansatz aktueller KI-Systeme zu verstehen.
- die Konzepte hinter dem bestärkenden Lernen zu verstehen.
- natürliche Sprache mit grundlegenden NLP-Techniken zu analysieren.
- Bilder und ihre Inhalte zu untersuchen.

## Kursinhalt

1. Geschichte der KI
  - 1.1 Historische Entwicklungen
  - 1.2 KI-Winter
  - 1.3 Expertensysteme
  - 1.4 Bedeutsame Fortschritte
2. Moderne KI-Systeme
  - 2.1 Schwache versus allgemeine KI
  - 2.2 Anwendungsbereiche

3. Bestärkendes Lernen
  - 3.1 Was ist bestärkendes Lernen?
  - 3.2 Markov-Ketten und Wertfunktion
  - 3.3 Zeitdifferenz und Q-Lernen
4. Verarbeitung natürlicher Sprache (NLP)
  - 4.1 Einführung in NLP und Anwendungsbereiche
  - 4.2 Grundlegende NLP-Techniken
  - 4.3 Vektorisierung von Daten
5. Computer Vision
  - 5.1 Pixel und Filter
  - 5.2 Feature-Erkennung
  - 5.3 Verzerrungen und Kalibrierung
  - 5.4 Semantische Segmentierung



**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Bear, F. / Barry, W. / Paradiso, M. (2006): Neuroscience: Exploring the brain. 3rd edition, Lippincott Williams and Wilkins, Baltimore, MD.
- Bird S. / Klein, E. / Loper, E. (2009): Natural language processing with Python. 2nd edition, O'Reilly, Sebastopol, CA.
- Chollet, F. (2017): Deep learning with Python. Manning, Shelter Island, NY.
- Fisher, R. B. et al (2016) : Dictionary of computer vision and image processing. John Wiley & Sons, Chichester.
- Geron, A. (2017): Hands-on machine learning with Scikit-Learn and TensorFlow. O'Reilly, Boston, MA.
- Goodfellow, I. / Bengio, Y. / Courville, A. (2016): Deep learning. MIT Press, Boston, MA.
- Grus, J. (2019): Data science from scratch: First principles with Python. O'Reilly, Sebastopol, CA.
- Jurafsky, D. / Martin, J. H. (2008): Speech and language processing. Prentice Hall, Upper Saddle River, NJ.
- Nilsson, N. (2009): The quest for artificial intelligence. Cambridge University Press, Cambridge.
- Russell, S. / Norvig, P. (2009): Artificial intelligence: A modern approach. 3rd edition, Pearson, Essex.
- Sutton, R. / Barto, A. (2018): Reinforcement learning: An introduction. 2nd edition, MIT Press, Boston, MA.
- Szelski, R. (2011): Computer vision: Algorithms and applications. 2nd edition, Springer VS, Wiesbaden.
- Szepesvári, C. (2010): Algorithms for reinforcement learning. Morgan & Claypool, San Rafael, CA.
- Wiering, M. / Otterlo, M. (2012): Reinforcement learning: State of the art. Springer, Berlin.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

## Standards der Informationssicherheit

Modulcode: DLBCSEISS\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Dr. Andreas Schmidt (Standards der Informationssicherheit)

### Kurse im Modul

- Standards der Informationssicherheit (DLBCSEISS01\_D)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Schriftliche Ausarbeitung: Fallstudie

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

- Aufbau der Informationssicherheitsstandards
- Informationssicherheitsmaßnahmen
- Informationssicherheits-Managementsystem (ISMS)
- Risikomanagement und -bewertung

**Qualifikationsziele des Moduls****Standards der Informationssicherheit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die allgemeine Struktur von Informationssicherheitsstandards zu verstehen.
- den normativen Inhalt von Frameworks und Standards zu verstehen.
- die erforderlichen Sicherheitsmaßnahmen zu kennen.
- bestehende Informationssicherheits-Managementsysteme zu analysieren.
- Informationssicherheits-Managementsysteme zu bewerten.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme aus dem Bereich IT & Technik

# Standards der Informationssicherheit

Kurscode: DLBCSEISS01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Informationssicherheit umfasst sowohl digitale als auch nicht digitale Informationen. Die Teilmenge IT-Security befasst sich nur mit elektronisch verarbeiteten, gespeicherten und übertragenen Informationen. Somit geht es bei der Informationssicherheit um die Sicherheit, die sich auf digitale und nicht digitale Werte eines Unternehmens bezieht.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die allgemeine Struktur von Informationssicherheitsstandards zu verstehen.
- den normativen Inhalt von Frameworks und Standards zu verstehen.
- die erforderlichen Sicherheitsmaßnahmen zu kennen.
- bestehende Informationssicherheits-Managementsysteme zu analysieren.
- Informationssicherheits-Managementsysteme zu bewerten.

## Kursinhalt

1. Einführung in die Informationssicherheit
  - 1.1 Grundlegende Definitionen, Sicherheitskonzepte und Ziele der Informationssicherheit
  - 1.2 Standards und regulatorische Rahmenbedingungen
  - 1.3 Sicherheitsstandards: ISO 27000-Familie und BSI-Standards
  - 1.4 Informationssicherheits-Managementsystem (ISMS)
2. Initiieren eines Informationssicherheits-Managementsystems
  - 2.1 Initiale Aufstellung für ein ISMS
  - 2.2 Analyse des Unternehmens
  - 2.3 Analyse des bestehenden ISMS und Bestimmung des Reifegrades
  - 2.4 Definition des ISMS-Anwendungsbereichs und der Sicherheitsrichtlinien

3. Implementierung des Informationssicherheits-Managementsystems
  - 3.1 Risikobewertung
  - 3.2 Statement of Applicability (SoA)
  - 3.3 Definition der Organisationsstruktur für die Informationssicherheit
  - 3.4 Dokumentenmanagement und Kommunikationsplan
  - 3.5 Definition von Maßnahmen und Prozeduren
4. Controlling des Informationssicherheits-Managementsystems
  - 4.1 Überwachung, Messung, Analyse und Auswertung
  - 4.2 Internes Audit
  - 4.3 Management Review
5. Verbesserung des Informationssicherheits-Managementsystems
  - 5.1 Betrachtung von Herausforderungen und Abweichungen
  - 5.2 Kontinuierliche Verbesserung
  - 5.3 Korrektive und präventive Aktionspläne
6. Maßnahmen des Informationssicherheits-Managementsystems
  - 6.1 Allgemeiner Aufbau der Maßnahmen
  - 6.2 Maßnahmen aus dem ISO 27001 - Annex A
  - 6.3 Verwaltung von Maßnahmen
  - 6.4 Bewertung der Effektivität von Maßnahmen

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Bundesamt für Sicherheit in der Informationstechnik (2012): Leitfaden Informationssicherheit. IT-Grundschutz kompakt. BSI, Bonn.
- Domnick, A. (2019): Informationssicherheit und Datenschutz. Handbuch für Praktiker und Begleitbuch zum T.I.S.P. 3., aktualisierte und erweiterte Auflage. Dpunkt Verlag, Heidelberg.
- Hanschke, I. (2019): Informationssicherheit und Datenschutz – einfach & effektiv. Integriertes Managementinstrumentarium systematisch aufbauen und verankern. Hanser, Carl, München.
- Sowa, A. (2017): Management der Informationssicherheit. Kontrolle und Optimierung. Springer Fachmedien, Wiesbaden.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

DLBCSEISS01\_D







# 5. Semester

---



## Seminar: Aktuelle Themen in Computer Science

Modulcode: DLBCSSCTCS\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b>	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	-----------------------------	---

### Modulverantwortliche(r)

N.N. (Seminar: Aktuelle Themen in Computer Science)

### Kurse im Modul

- Seminar: Aktuelle Themen in Computer Science (DLBCSSCTCS01\_D)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Schriftliche Ausarbeitung: Seminararbeit

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

Dieses Seminar befasst sich mit aktuellen Themen der Informatik. Die Studierenden beschäftigen sich innerhalb einer Teildisziplin ihrer Wahl vertieft mit einem bestimmten Thema.

**Qualifikationsziele des Moduls****Seminar: Aktuelle Themen in Computer Science**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ein bestimmtes Thema aus dem Bereich der Informatik vertieft und aufschlussreich zu diskutieren.
- über ein bestimmtes Informatik-Thema im Hinblick auf wichtige Eigenschaften, Zusammenhänge und Erkenntnisse in Form eines Forschungsaufsatzes zu schreiben.
- die Grundlagen wissenschaftlichen Arbeitens anzuwenden und im Rahmen einer Seminararbeit umzusetzen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung.

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik.

## Seminar: Aktuelle Themen in Computer Science

Kurscode: DLBCSSCTCS01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

### Beschreibung des Kurses

Dieses Seminar ist eine Gelegenheit für die Studierenden, das breite Wissen zu vertiefen, das sie in den vorangegangenen Kursen des Studiengangs erworben haben. Die Studierenden wählen ein Thema von spezifischem individuellem Interesse, das mit einer Teildisziplin der Informatik verbunden ist. Wenn ein Studierender beispielsweise an der Anwendung künstlicher Intelligenz in einem bestimmten Kontext interessiert ist, kann die Ausarbeitung kontextspezifischer Anwendungsfälle aus einer Literaturübersicht das Thema des Aufsatzes sein. Das Feedback der Tutorin oder des Tutors hilft den Studierenden, eventuelle Schwächen im wissenschaftlichen Schreiben und in der akademischen Arbeit zu bearbeiten und die Studierenden auf die Abfassung ihrer Bachelorarbeit vorzubereiten.

### Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ein bestimmtes Thema aus dem Bereich der Informatik vertieft und aufschlussreich zu diskutieren.
- über ein bestimmtes Informatik-Thema im Hinblick auf wichtige Eigenschaften, Zusammenhänge und Erkenntnisse in Form eines Forschungsaufsatzes zu schreiben.
- die Grundlagen wissenschaftlichen Arbeitens anzuwenden und im Rahmen einer Seminararbeit umzusetzen.

### Kursinhalt

- Die Informatik ist ein breites Fachgebiet mit vielen sehr unterschiedlichen Facetten, je nach spezifischer Teildisziplin. Dieses Seminar geht auf diese Vielfalt ein, indem es aktuelle Trends im Rahmen individuell erstellter Texte aufgreift. Studierende sollen zu diesem Zweck eine Seminararbeit verfassen. Mögliche Themen sind Java- und Webentwicklung, Datenmodellierung und Datenbanksysteme, Requirements Engineering und Kerndisziplinen der Informatik wie Betriebssysteme, Rechnernetze, verteilte Systeme, Algorithmen, Datenstrukturen und Programmiersprachen.

**Literatur**

**Pflichtliteratur**

**Weiterführende Literatur**

- Brookshear, G. / Bylow, D. (2014): Computer science: An overview. 12th edition, Pearson, Boston, MA.
- Gruhn, V. / Striemer, R. (Eds.). (2018): The essence of software engineering. Springer, Cham.
- Springer. (n.d.): Lecture Notes in Computer Science. Springer, Heidelberg.
- Tardos, E. (Ed.). (n.d.): Journal of the ACM.



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Seminar
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Seminararbeit

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

DLBCSSCTCS01\_D

## Advanced Data Analysis

Modulcode: DLBDEDA1\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

N.N. (Advanced Data Analysis)

### Kurse im Modul

- Advanced Data Analysis (DLBDEDA01\_D)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Klausur, 90 Minuten

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

- Analyse der Unternehmensleistung
- Text-Mining
- Web- und Social Media-Analyse
- Experimentieren und Testen

**Qualifikationsziele des Moduls****Advanced Data Analysis**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- wichtige Designüberlegungen für geschäftliche KPIs zu identifizieren.
- verschiedene Themen der Geschäftsprozessanalyse zu erläutern.
- etablierte Techniken zur Webdatenanalyse zu nutzen.
- analytische Ansätze für Text Mining und semantische Analyse zu verstehen.
- relevante Fragen in der Social-Media-Analyse zu verdeutlichen.
- die Techniken und Methoden zum Experimentieren und Testen anzuwenden.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Data Science & Artificial Intelligence

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Advanced Data Analysis

Kurscode: DLBDESDA01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Dieser Kurs führt in verschiedene fortgeschrittene analytische Themen von praktischer Relevanz ein. Die behandelten Themenbereiche reichen von der Messung und Analyse der Unternehmensleistung, Text Mining, Web- und Social Media-Analytik bis hin zu aktuellen Trends im experimentellen Design und Aufbau. Entlang dieser Reise werden Themen wie die Gestaltung von Leistungskennwerten - Key Performance Indicators (KPIs), Geschäftsprozessanalyse, Worthäufigkeits- und semantische Analyse, Datenwissenschaft zu „Clickstreams“, Social Media Interaktionen und mehrarmige Banditentest Algorithmen behandelt.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- wichtige Designüberlegungen für geschäftliche KPIs zu identifizieren.
- verschiedene Themen der Geschäftsprozessanalyse zu erläutern.
- etablierte Techniken zur Webdatenanalyse zu nutzen.
- analytische Ansätze für Text Mining und semantische Analyse zu verstehen.
- relevante Fragen in der Social-Media-Analyse zu verdeutlichen.
- die Techniken und Methoden zum Experimentieren und Testen anzuwenden.

## Kursinhalt

1. Analytik der Unternehmensleistung
  - 1.1 Überlegungen zum KPI-Design
  - 1.2 Gängige Leistungsindikatoren für Unternehmen
  - 1.3 Geschäftsprozessanalyse – Business process mining
2. Text-Analyse
  - 2.1 Wort- und Dokumentfrequenz (TF-IDF)
  - 2.2 Semantische Analyse
3. Web-Analytik
  - 3.1 Web-Metriken
  - 3.2 Clickstream-Analyse
  - 3.3 Empfehlungsdienste

4. Social Network Mining
  - 4.1 Einführung in die Analytik der sozialen Medien
  - 4.2 "Ausbeutung" von gängigen Plattformen für soziale Medien
5. Tests und Experimente
  - 5.1 Praktische A/B-Prüfung
  - 5.2 Multivariate Tests
  - 5.3 Tests mit mehrarmigen Banditen Algorithmen

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Hapke, H., Howard, C., & Lane, H. (2019). Natural language processing in action. Shelter Island, NY: Manning Publications.
- Kaushik, A. (2009). Web analytics 2.0: The art of online accountability and science of customer centricity. Hoboken, NJ: Sybex.
- Klassen, M., & Russell, M. A. (2019). Mining the social web (3rd ed.). Sebastopol, CA: O'Reilly Media.
- Marr, B. (2012). Key Performance Indicators (KPI). Boston, MA: Pearson.
- Neely, A. (Ed.). (2011). Business performance measurement: Unifying theory and integrating practice (2nd ed.). Cambridge: Cambridge University Press.
- Ojeda, T., Bilbro, R., & Bengfort, B. (2018). Applied text analysis with Python. Sebastopol, CA: O'Reilly Media.
- Parmenter, D. (2015). Key performance indicators: Developing, implementing, and using winning KPIs (3rd ed.). Chichester: John Wiley & Sons.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBDSEDA01\_D



## Projekt: Data Analysis

Modulcode: DLBDEDA2\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof. Dr. Frank Passing (Projekt: Data Analysis)

### Kurse im Modul

- Projekt: Data Analysis (DLBDEDA02\_D)

### Art der Prüfung(en)

#### Modulprüfung

Studienformat: Fernstudium  
Portfolio

#### Teilmodulprüfung

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### Lehrinhalt des Moduls

Transfer von methodischem Wissen zur Umsetzung von Anwendungsfällen der Analytik in der realen Welt aus den oben genannten Problembereichen.

**Qualifikationsziele des Moduls**

**Projekt: Data Analysis**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einen analytischen Anwendungsfall aus der realen Welt zu formulieren und zu implementieren.
- die Eignung verschiedener möglicher Ansätze im Hinblick auf die Projektaufgabe zu analysieren.
- erworbenes analytisches Spezialwissen auf reale Anwendungsfälle zu übertragen.
- relevante Designentscheidungen aus dem gegebenen Projektumfeld abzuleiten.
- geeignete Entscheidungen in Bezug auf Umsetzungsalternativen zu treffen.
- geeignete Ressourcen auszuwählen.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Data Science & Artificial Intelligence

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Projekt: Data Analysis

Kurscode: DLBDSEDA02\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Der Schwerpunkt dieses Kurses liegt auf der Implementierung eines realen, fortgeschrittenen analytischen Anwendungsfalles in Form eines Studierendenprojekts. Zu den primären Themenbereichen dieser praktischen Arbeit gehören Business Performance Analytics, Text Mining, Web- und Social Analytics sowie Experimentieren und Testen. Ziel ist es, dass die Studierenden zeigen können, dass sie das in der Advanced Data Analysis (DLBDSEDA01) erworbene theoretische Wissen auf ein Implementierungsszenario übertragen können, das die Projektarbeit in einem professionellen datenwissenschaftlichen Umfeld nachahmt.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einen analytischen Anwendungsfall aus der realen Welt zu formulieren und zu implementieren.
- die Eignung verschiedener möglicher Ansätze im Hinblick auf die Projektaufgabe zu analysieren.
- erworbenes analytisches Spezialwissen auf reale Anwendungsfälle zu übertragen.
- relevante Designentscheidungen aus dem gegebenen Projektumfeld abzuleiten.
- geeignete Entscheidungen in Bezug auf Umsetzungsalternativen zu treffen.
- geeignete Ressourcen auszuwählen.

## Kursinhalt

- Dieser Kurs behandelt die praktische Umsetzung der im Kurs Advanced Data Analytics (DLBDSEDA01) behandelten Ansätze und Techniken in einer projektorientierten Umgebung. Alle Teilnehmenden müssen einen Projektbericht erstellen, in dem ihre Arbeit detailliert und dokumentiert wird. Die Projektaufgaben werden aus einer Liste ausgewählt oder von den Studierenden in Absprache mit dem Tutor vorgeschlagen.

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Hapke, H., Howard, C., & Lane, H. (2019). Natural language processing in action. Shelter Island, NY: Manning Publications.
- Kaushik, A. (2009). Web analytics 2.0: The art of online accountability and science of customer centricity. Hoboken, NJ: Sybex.
- Klassen, M., & Russell, M. A. (2019). Mining the social web (3rd ed.). Sebastopol, CA: O'Reilly Media.
- Marr, B. (2012). Key Performance Indicators (KPI). Boston, MA: Pearson.
- Neely, A. (Ed.). (2011). Business performance measurement: Unifying theory and integrating practice (2nd ed.). Cambridge: Cambridge University Press.
- Ojeda, T., Bilbro, R., & Bengfort, B. (2018). Applied text analysis with Python. Sebastopol, CA: O'Reilly Media.
- Parmenter, D. (2015). Key performance indicators: Developing, implementing, and using winning KPIs (3rd ed.). Chichester: John Wiley & Sons.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Portfolio

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input checked="" type="checkbox"/> Folien
<input type="checkbox"/> Musterklausur	

DLBDEDA02\_D

# Cloud Computing

Modulcode: DLBDSCC\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 5	<b>Zeitaufwand Studierende</b> 150 h
----------------------------------	--	---------------------	------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Christian Müller-Kett (Cloud Computing)

## Kurse im Modul

- Cloud Computing (DLBDSCC01\_D)

## Art der Prüfung(en)

### Modulprüfung

Studienformat: Fernstudium  
Klausur, 90 Minuten

### Teilmodulprüfung

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

## Lehrinhalt des Moduls

- Grundlagen des Cloud Computing
- Relevante Basistechnologien für Cloud Computing
- Einführung in Serverless Computing
- Etablierte Cloud-Plattformen
- Cloud-Angebote für Datenwissenschaft und -analyse

**Qualifikationsziele des Moduls****Cloud Computing**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen von Cloud Computing und Cloud-Service-Modellen zu verstehen.
- technologische Voraussetzungen zu erkennen, die aktuellen Cloud-Angeboten zugrunde liegen.
- die Prinzipien des Serverless Computing darzulegen.
- Merkmale der etablierten Cloud-Angebote zu analysieren.
- Cloud-Optionen für Datenwissenschaft und maschinelles Lernen zu beschreiben.

**Bezüge zu anderen Modulen im Studiengang**

Ist Grundlage für alle weiteren Module aus dem Bereich Data Science & Artificial Intelligence.

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik



# Cloud Computing

Kurscode: DLBDSCC01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Viele der jüngsten Fortschritte in der Datenwissenschaft, insbesondere beim maschinellen Lernen und bei der künstlichen Intelligenz, beruhen auf umfassender Datenspeicherung und Rechenleistung. Cloud Computing ist eine Möglichkeit, diese Leistung auf skalierbare Weise und ohne beträchtliche Vorabinvestitionen in Hardware- und Software-Ressourcen bereitzustellen. Dieser Kurs führt in den Bereich des Cloud Computing zusammen mit seinen technologischen Voraussetzungen ein. Darüber hinaus werden die neuesten Fortschritte, wie Serverless Computing und Speicherung, veranschaulicht. Schließlich wird ein gründlicher Überblick über beliebte Cloud-Angebote, insbesondere im Hinblick auf Analysemöglichkeiten, gegeben.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen von Cloud Computing und Cloud-Service-Modellen zu verstehen.
- technologische Voraussetzungen zu erkennen, die aktuellen Cloud-Angeboten zugrunde liegen.
- die Prinzipien des Serverless Computing darzulegen.
- Merkmale der etablierten Cloud-Angebote zu analysieren.
- Cloud-Optionen für Datenwissenschaft und maschinelles Lernen zu beschreiben.

## Kursinhalt

1. Einführung in Cloud Computing
  - 1.1 Grundlagen des Cloud Computing
  - 1.2 Cloud-Service-Modelle
  - 1.3 Nutzen und Risiken
2. Technologische Voraussetzungen
  - 2.1 Virtualisierung und Containerisierung
  - 2.2 Speichertechnik
  - 2.3 Netzwerke und RESTful-Dienste

3. Serverloses Rechnen
  - 3.1 Einführung in Serverless Computing
  - 3.2 Vorteile
  - 3.3 Einschränkungen
4. Etablierte Cloud-Plattformen
  - 4.1 Google-Cloudplattform
  - 4.2 Amazon-Webdienste
  - 4.3 Microsoft Azure
5. Datenwissenschaft in der Cloud
  - 5.1 Google-Dienste für Datenwissenschaft und maschinelles Lernen
  - 5.2 Amazon Web Services für Datenwissenschaft und maschinelles Lernen
  - 5.3 Microsoft Azure für Datenwissenschaft und maschinelles Lernen

## Literatur

### Pflichtliteratur

#### Weiterführende Literatur

- Chapin, J. / Roberts, M. (2017): What is serverless? O'Reilly Media, Sebastopol, CA.
- Goessling, S. / Jackson, K. L. (2018): Architecting cloud computing solutions. Packt Publishing, Birmingham.
- Kavis, M. J. (2014): Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, and IaaS). Wiley, Hoboken, NJ.
- Mahmood, Z. / Puttini, R. / Erl, T. (2013): Cloud computing: Concepts, technology & architecture. Prentice Hall, Boston, MA.
- Rafaels, R. (2018): Cloud computing. 2nd edition, CreateSpace Independent Publishing Platform, Scotts Valley, CA.
- Sehgal, N. K. / Bhatt, P. C. P. (2018): Cloud computing: Concepts and practices. Springer, Cham.
- Zonooz, P. et al (2018): Cloud native architectures. Packt Publishing, Birmingham.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBDSCC01\_D

# IT-Sicherheitsberatung

Modulcode: DLBCSEEISC\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ DLBCSEEISC01_D oder DLBCSEEISC01_E</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	---	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

N.N. (Technische und betriebliche IT-Sicherheitskonzeptionen) / N.N. (Projekt: Einsatz und Konfiguration von SIEM-Systemen)

## Kurse im Modul

- Technische und betriebliche IT-Sicherheitskonzeptionen (DLBCSEEISC01\_D)
- Projekt: Einsatz und Konfiguration von SIEM-Systemen (DLBCSEEISC02\_D)

## Art der Prüfung(en)

### Modulprüfung

### Teilmodulprüfung

Technische und betriebliche IT-Sicherheitskonzeptionen

- Studienformat "Fernstudium": Klausur, 90 Minuten

Projekt: Einsatz und Konfiguration von SIEM-Systemen

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

### **Lehrinhalt des Moduls**

#### **Technische und betriebliche IT-Sicherheitskonzeptionen**

- Netzwerkanalyse und -auswertung
- Schutz-Profile
- Systeme der Intrusion Detection
- Netzwerk-Überwachung
- Sicherheitsinformationen und Ereignismanagement (SIEM)
- IT-Sicherheitsevaluierung und -bewertung

#### **Projekt: Einsatz und Konfiguration von SIEM-Systemen**

Dieser Projektkurs vermittelt den Studierenden praktische Erfahrungen mit der anspruchsvollen Aufgabe der Implementierung eines SIEM-Tools (Security Incident Event Management) in eine Unternehmens-IT-Umgebung. Die Studierenden müssen praktische Aspekte wie verschiedene Datenquellen, Datenfusion und Analysemethoden und -verarbeitung von große Datenmengen sowie Einschränkungen durch die Datenverfügbarkeit und unterschiedlichste Datenformate berücksichtigen:

**Qualifikationsziele des Moduls****Technische und betriebliche IT-Sicherheitskonzeptionen**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-Systeme und -Netzwerke zu analysieren und zu bewerten und Vulnerabilitäten aufzudecken.
- unternehmensspezifische "Schutzprofile" zu entwickeln.
- Tools für sensorbasierte Netzwerküberwachung, Intrusion Detection und Reaktionen darauf zu entwerfen und zu implementieren.
- "Big Data"-Fusionsmechanismen zu verwenden, den Sicherheitsstatus des IT-Systems und den Netzwerksicherheitsstatus zu bewerten und zu beurteilen und Maßnahmen zur Reaktion auf Vorfälle einzuleiten.
- den Sicherheitsstatus von IT-Systemen und Netzwerken zu bewerten und Ratschläge für Verbesserungen zu geben.

**Projekt: Einsatz und Konfiguration von SIEM-Systemen**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Herausforderungen bei der Integration eines SIEM in eine bestehende Unternehmens-IT-Infrastruktur zu verstehen.
- die technischen Grenzen zu bewerten, die mit dem Projekt der Implementierung und dem Betrieb eines SIEM verbunden sind.
- die für eine zuverlässige Ausführung des SIEM-Tools erforderlichen Komponenten zur Intrusions-Erkennung und -überwachung zu identifizieren.
- die Anforderungen hinsichtlich Datenerfassung, Datenfusion, -analyse und -verarbeitung zu analysieren.
- die Abweichung vom Normverhalten in IT-Systemen / Netzwerken zu identifizieren.
- eine eingehende Untersuchung von Malware-Proben einzuleiten und relevante Reaktionsstrategien anzuwenden - einschließlich automatisierter Antworten.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Technische und betriebliche IT-Sicherheitskonzeptio- nen

Kurscode: DLBCSEEISC01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

IT-Systeme und Netzwerke, die hochsensible Informationen und Daten enthalten und verarbeiten, sowie IT-Infrastruktur zur Unterstützung geschäftskritischer Prozesse oder nationaler kritischer Infrastrukturen erfordern höhere Sicherheitsmechanismen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. Basierend auf spezifischen "Schutzprofilen" müssen hoch entwickelte Tools, Mechanismen und Verfahren entworfen, implementiert, konfiguriert und betrieben werden. Mit diesem Kurs werden Studierende in der Lage sein, die gegebene IT-Infrastruktur zu bewerten, das Sicherheitsdesign neuer IT-Systeme und Netzwerke durch die Entwicklung spezifischer Schutzprofile zu unterstützen, und zu bewerten, welche technischen und betrieblichen Sicherheitsmaßnahmen und Anwendungen erforderlich sind und wie diese im Unternehmen integriert, konfiguriert und betrieben werden.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-Systeme und -Netzwerke zu analysieren und zu bewerten und Vulnerabilitäten aufzudecken.
- unternehmensspezifische "Schutzprofile" zu entwickeln.
- Tools für sensorbasierte Netzwerküberwachung, Intrusion Detection und Reaktionen darauf zu entwerfen und zu implementieren.
- "Big Data"-Fusionsmechanismen zu verwenden, den Sicherheitsstatus des IT-Systems und den Netzwerksicherheitsstatus zu bewerten und zu beurteilen und Maßnahmen zur Reaktion auf Vorfälle einzuleiten.
- den Sicherheitsstatus von IT-Systemen und Netzwerken zu bewerten und Ratschläge für Verbesserungen zu geben.

## Kursinhalt

1. Netzwerkanalyse und -auswertung
  - 1.1 Schichtspezifische Bedrohungen und Schwachstellen
  - 1.2 Daten-Fluss, Interdependenzen und Interrelationen
  - 1.3 Überprüfung und Erkennen von Schwachstellen
  - 1.4 Unterstützende Tools und Techniken



2. Schutz-Profile
  - 2.1 Referenzarchitektur, Technologie und Netzwerkbetrieb
  - 2.2 Risikobewertung, Restrisiko und Risikomanagement
  - 2.3 Sicherheitsanforderungen und Schutzmaßnahmen
  - 2.4 Sicherheitsbewertung von IT-Sicherheitsprodukten
  - 2.5 Akkreditierung von IT-Systemen und Netzwerken
3. Systeme der Intrusion Detection
  - 3.1 Erkennungsstrategie,
  - 3.2 Datenquellen, Sensoren
  - 3.3 Analytik
  - 3.4 Indikatoren für Kompromittierungen
4. Netzwerk-Überwachung
  - 4.1 Systeme zum Schutz vor Bedrohungen
  - 4.2 Technologie drahtloser Sensornetzwerke
  - 4.3 Austausch von Bedrohungsinformationen
5. Sicherheitsinformationen und Ereignismanagement (SIEM)
  - 5.1 Technische und betriebliche Daten-Quellen
  - 5.2 DATA-Fusion
  - 5.3 Normverhalten von Netzwerken
  - 5.4 Analyse großer Datenmengen - Übertragung technischer Daten in operative Informationen
  - 5.5 IT- Sicherheitslage und Lagebewusstsein
  - 5.6 Strategien zur Reaktion auf Vorfälle und automatisierte Gegenmaßnahmen
6. IT-Sicherheitsevaluierung und -bewertung
  - 6.1 IT-Sicherheits-Metriken
  - 6.2 Bewertung der IT-Sicherheit

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Bundesamt Für Sicherheit in der Informationstechnik und ConSecur GmbH - Einführung von Intrusion-Detection-Systemen, 31. Oktober 2002 - [www.bsi.bund.de](http://www.bsi.bund.de)
- Wolfgang Röck, Netzwerksicherheit und Intrusion Detection: Implementierung und Evaluierung eines Intrusion Detection Systems auf Basis des Open Source Systems Snort (Deutsch) Taschenbuch – 30. Januar 2009
- IT-Grundschutz Profiles - Structural Description - COMMUNITY DRAFT - © Federal Office for Information Security (BSI) 2018
- Martin Kappes, Netzwerk- und Datensicherheit ISBN: 3658161264 mEAN: 9783658161262 Eine praktische Einführung. 3., akt. und erweiterte Aufl. 2019
- David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask, Security Information and Event Management (SIEM) Implementation ©2011 The MacGraw-Hill Companies ISBN:978-0-07-170108-2
- Lance Hayden, Publication: Cover Image. · Book, IT Security Metrics: A PracticalFramework for Measuring Security & Protecting Data. 1st McGraw-Hill Education Group ©2010
- Chris McNab, Network Security Assessment

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

## Projekt: Einsatz und Konfiguration von SIEM-Systemen

Kurscode: DLBCSEEISC02\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSEEISC01_D oder DLBCSEEISC01_E

### Beschreibung des Kurses

Dieser Projektkurs vermittelt den Studierenden praktische Erfahrungen mit der anspruchsvollen Aufgabe der Implementierung eines SIEM-Tools (Security Incident Event Management) in eine Unternehmens-IT-Umgebung. Die Studierenden müssen praktische Aspekte wie verschiedene Datenquellen, Datenfusion und Analysemethoden und -verarbeitung von große Datenmengen sowie Einschränkungen durch die Datenverfügbarkeit und unterschiedlichste Datenformate berücksichtigen. Darüber hinaus stehen die Studierenden vor der Herausforderung, technische Daten in betriebliche Informationen zu übertragen, um die entsprechenden Gegenmaßnahmen einzuleiten. Durch diesen Kurs erhalten die Studenten einen ganzheitlichen Überblick über die Integration eines SIEM in eine Unternehmens-IT-Infrastruktur, sowie deren Anwendungen und Dienste.

### Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Herausforderungen bei der Integration eines SIEM in eine bestehende Unternehmens-IT-Infrastruktur zu verstehen.
- die technischen Grenzen zu bewerten, die mit dem Projekt der Implementierung und dem Betrieb eines SIEM verbunden sind.
- die für eine zuverlässige Ausführung des SIEM-Tools erforderlichen Komponenten zur Intrusions-Erkennung und -überwachung zu identifizieren.
- die Anforderungen hinsichtlich Datenerfassung, Datenfusion, -analyse und -verarbeitung zu analysieren.
- die Abweichung vom Normverhalten in IT-Systemen / Netzwerken zu identifizieren.
- eine eingehende Untersuchung von Malware-Proben einzuleiten und relevante Reaktionsstrategien anzuwenden - einschließlich automatisierter Antworten.

### Kursinhalt

- Dieser Projektkurs konzentriert sich auf praktische Aspekte der Implementierung eines SIEM in einer Unternehmens-IT-Infrastrukturumgebung. Die Studierenden beginnen mit einem ausgewählten Anwendungsfall und SIEM-System und evaluieren dann die Anforderungen, die erfüllt werden müssen, damit das SIEM-Systems als Teil eines Unternehmens-IT-Systems / Netzwerkes eingesetzt werden kann. Die Studierenden müssen die Anforderungen in Bezug auf Sensoren, Netzwerküberwachung, Intrusion Detection, Datenfusion, Big Data Analytics und die Umsetzung technischer Daten in betriebliche Informationen evaluieren.

- Auf der Grundlage der verfügbaren Informationen werden geeignete Gegenmaßnahmen - einschließlich automatisierter Gegenmaßnahmen - identifiziert und verarbeitet.
- Alle relevanten Artefakte und Überlegungen werden von den Studierenden in einem Projektbericht dokumentiert.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask, Security Information and Event Management (SIEM) Implementation ©2011 The MacGraw-Hill Companies ISBN:978-0-07-170108-2
- Whitepaper: Die sieben Kernfunktionen analysegestützter SIEM-Lösungen - [www.splunk.com](http://www.splunk.com)
- H. B. Mitchell Multi-Sensor Data Fusion: An Introduction – Springer Verlag ISBN: 978-3642090677
- Al-Sakib Khan Pathan The State of the Art in Intrusion Prevention and Detection – CRC Press, Taylor&Francis Group

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input checked="" type="checkbox"/> Folien
<input type="checkbox"/> Musterklausur	

# Social Engineering

Modulcode: DLBCSEESE\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ DLBCSEESE01_D oder DLBCSEESE01_E</li> <li>▪ keine</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	---	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

N.N. (Social Engineering und Insider Threats) / N.N. (Projekt: Social Engineering)

## Kurse im Modul

- Social Engineering und Insider Threats (DLBCSEESE01\_D)
- Projekt: Social Engineering (DLBCSEESE02\_D)

## Art der Prüfung(en)

### Modulprüfung

### Teilmodulprüfung

Social Engineering und Insider Threats

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Fallstudie

Projekt: Social Engineering

- Studienformat "Fernstudium": Projektpräsentation

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### **Lehrinhalt des Moduls**

#### **Social Engineering und Insider Threats**

- Methoden des Social Engineering
- Rechtliche Aspekte des Social Engineering
- Compliance, Verhaltenskodex
- Erkennung von Insider-Bedrohungen
- Sicherheitspolitik und -vorschriften
- Nationale und internationale Zusammenarbeit und Informationsaustausch

#### **Projekt: Social Engineering**

- Methoden des Social Engineering
- Rechtliche Aspekte des Social Engineering
- Compliance, Verhaltenskodex
- Erkennung von Insider-Threats
- Sicherheitspolitik und -vorschriften
- Nationale und internationale Zusammenarbeit und Informationsaustausch



**Qualifikationsziele des Moduls****Social Engineering und Insider Threats**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Social-Engineering-Methoden gegenüber IT-Systemen und Netzwerken und erkennen Schwachstellen im eigenen Unternehmen zu analysieren und zu bewerten.
- Unternehmensspezifische, technische und organisatorische Sicherheitsrichtlinien und -vorschriften zu bewerten.
- Tools für die Netzwerküberwachung zu entwerfen und zu implementieren, um die Anwendung von Sicherheitsrichtlinien und -vorschriften zu erkennen und zu protokollieren.
- "Big Data"-Fusions- und maschinelle Lernmechanismen zur Bewertung und Beurteilung des IT-Systemnetzwerks sowie des Sicherheitsstatus von Benutzern und Administratoren und zur Entscheidung und Einleitung von Reaktionsmaßnahmen einzusetzen, um sich von Social Engineering und durch Insider-Bedrohungen verursachten Vorfällen zu erholen.
- den Sicherheitsstatus und das Sicherheitsbewusstsein im Unternehmen auf allen Ebenen zu bewerten und Ratschläge für Verbesserungen zu geben.

**Projekt: Social Engineering**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Bedeutung des "menschlichen Faktors" im Hinblick auf die Sicherheit von IT-Systemen und Netzwerken in Unternehmen anzuerkennen und die rechtlichen Normen im Hinblick auf Social Engineering und die Erkennung von Insider-Bedrohungen zu berücksichtigen.
- den Sicherheitsrahmen zu analysieren und zu bewerten und Sicherheitslücken und -defizite zu ermitteln.
- organisatorische, technische und sicherheitstechnische Richtlinien und Vorschriften zu entwickeln und umzusetzen.
- Kampagnen zur Förderung des Sicherheitsbewusstseins zu entwickeln und durchzuführen, um die Widerstandsfähigkeit gegen die Anwendung von Methoden des Social Engineering zu erhöhen.
- mit verschiedenen Interessengruppen wie nationalen Sicherheitsbehörden, Sicherheitsunternehmen und Internetdiensteanbietern zusammenzuarbeiten.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

## Social Engineering und Insider Threats

Kurscode: DLBCSEESE01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

### Beschreibung des Kurses

IT-Systeme und Netzwerke, die hochsensible Informationen und Daten enthalten und verarbeiten, sowie IT-Infrastruktur zur Unterstützung geschäftskritischer Prozesse oder nationaler kritischer Infrastrukturen sind für Angreifer von großem Interesse, um Informationen zu erlangen (Cyber-Spionage), Informationen und Daten zu manipulieren oder zu zerstören sowie grundlegende Funktionen und Dienste zu unterbrechen, indem sie diese Systeme und Unternehmen kompromittieren. Ein Angriffsvektor richtet sich an die Benutzer und Betreiber, um diese Personen als Mithelfer zu missbrauchen, um Sicherheitsrichtlinien und Vorschriften zu brechen. Social Engineering oder soziale Manipulation wird von Gegnern häufig eingesetzt, um an die notwendigen Informationen zu gelangen, um IT-Infrastrukturen zu kompromittieren und ihre spezifischen Ziele zu erreichen. Der Einsatz von Methoden des Social Engineering kommt der sogenannten "Insider-Bedrohung" sehr nahe. Personen aus dem Inneren der Organisation handeln aus verschiedenen Gründen gegen die Sicherheitspolitik und -vorschriften ihres eigenen Unternehmens. Rache, Unzufriedenheit oder manchmal auch kriminelle Absichten sind Gründe für ein solches Verhalten. Eine Kombination aus Social Engineering und "feindlichen Insidern" ist ein Ass für alle Gegner. Daher müssen technische und organisatorische Maßnahmen entwickelt und umgesetzt werden, um solche Bedrohungen abzuwenden. Mit diesem Kurs sind die Studierenden in der Lage, Methoden des Social Engineering zu erkennen und Insider-Bedrohungen zu identifizieren. Sie sind in der Lage, präventive Sicherheitsrichtlinien und -vorschriften sowie reaktionsfähige Sicherheitsmaßnahmen zu entwickeln und umzusetzen, um diesen Bedrohungen zu begegnen.

**Kursziele**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Social-Engineering-Methoden gegenüber IT-Systemen und Netzwerken und erkennen Schwachstellen im eigenen Unternehmen zu analysieren und zu bewerten.
- Unternehmensspezifische, technische und organisatorische Sicherheitsrichtlinien und -vorschriften zu bewerten.
- Tools für die Netzwerküberwachung zu entwerfen und zu implementieren, um die Anwendung von Sicherheitsrichtlinien und -vorschriften zu erkennen und zu protokollieren.
- "Big Data"-Fusions- und maschinelle Lernmechanismen zur Bewertung und Beurteilung des IT-Systemnetzwerks sowie des Sicherheitsstatus von Benutzern und Administratoren und zur Entscheidung und Einleitung von Reaktionsmaßnahmen einzusetzen, um sich von Social Engineering und durch Insider-Bedrohungen verursachten Vorfällen zu erholen.
- den Sicherheitsstatus und das Sicherheitsbewusstsein im Unternehmen auf allen Ebenen zu bewerten und Ratschläge für Verbesserungen zu geben.

**Kursinhalt**

1. Methoden des Social Engineering
  - 1.1 Phishing, Spear Phishing und Dynamite Phishing
  - 1.2 Quid pro quo, Köder (Baiting), Medienköder (Media Dropping)
  - 1.3 Scareware, Betrugsmasche CEO-Fraud
  - 1.4 Pretexting, Tailgating
2. Rechtliche Aspekte des Social Engineering
  - 2.1 Compliance, Verhaltenskodex
  - 2.2 Identitätsdiebstahl
  - 2.3 Datenschutz
3. Detektion von Innentätern
  - 3.1 Techniken des Data Mining
  - 3.2 Methoden des Machine Learning
  - 3.3 Umfassendes Framework für die Detektion von und Reaktion bei Innentätern
  - 3.4 Tools für die Selbstbeurteilung
  - 3.5 Organisatorische Maßnahmen und Awareness
4. Sicherheitsrichtlinien und -vorschriften
  - 4.1 Organisatorisches Framework, Compliance, Verhaltenskodex
  - 4.2 Training und Awareness
  - 4.3 Schutz vertraulicher Informationen
  - 4.4 Sicherheitsüberwachung und Störfallreaktion

5. Nationale/r und internationale/r Zusammenarbeit und Informationsaustausch
  - 5.1 Zusammenarbeit mit Internet Service Providern (ISP) und Vertretern der IT-Sicherheit
  - 5.2 Austauschplattformen und Foren für Tactics, Techniques und Procedures (TTP) und Best Practices
  - 5.3 Zusammenarbeit mit nationalen Sicherheitsbehörden

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited, Brisbane.
- Company: TrustedSec. (Internet DEMO Version to subscribe)
- Hadnagy, C. (2012): Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe, MITP-Verlags GmbH & Co. KG, Frechen.
- Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, Oxford.
- Kennedy, D.: The Social-Engineer Toolkit (SET)
- Menger, A. (2016): IT-Sicherheit und Social Engineering. Grundlagen, Erscheinungsformen und Schutzmöglichkeiten. Hochschule Osnabrück.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# Projekt: Social Engineering

Kurscode: DLBCSEESE02\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSEESE01_D oder DLBCSEESE01_E

## Beschreibung des Kurses

Dieser Projektkurs vermittelt den Studierenden praktische Erfahrungen mit der anspruchsvollen Aufgabe, Social Engineering-Angriffe zu verhindern und zu kontern und die Insider-Bedrohung für die IT-Systeme und -Netzwerke von Unternehmen zu beseitigen oder zumindest zu mindern. Die Studierenden müssen praktische Aspekte sozialer und psychologischer Herausforderungen - den so genannten "Human Factor" - sowie die Anwendung technischer Toolkits zur Erkennung von Angriffen berücksichtigen, die durch Social-Engineering-Methoden gesteuert oder von feindlichen Insidern verursacht werden. Im Rahmen dieses Kurses erhalten die Teilnehmer einen vollständigen Überblick über organisatorische, technische und verfahrenstechnische Maßnahmen, indem sie die Landschaft der Bedrohungsvektoren analysieren, Schwachstellen und Sicherheitslücken im Unternehmen identifizieren und praktische Sicherheitsrichtlinien und -vorschriften, einschließlich Kampagnen zur Förderung des Sicherheitsbewusstseins, entwickeln und umsetzen, um durch Social Engineering und Insider-Bedrohungen verursachte Vorfälle zu verhindern und sich von ihnen zu erholen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Bedeutung des "menschlichen Faktors" im Hinblick auf die Sicherheit von IT-Systemen und Netzwerken in Unternehmen anzuerkennen und die rechtlichen Normen im Hinblick auf Social Engineering und die Erkennung von Insider-Bedrohungen zu berücksichtigen.
- den Sicherheitsrahmen zu analysieren und zu bewerten und Sicherheitslücken und -defizite zu ermitteln.
- organisatorische, technische und sicherheitstechnische Richtlinien und Vorschriften zu entwickeln und umzusetzen.
- Kampagnen zur Förderung des Sicherheitsbewusstseins zu entwickeln und durchzuführen, um die Widerstandsfähigkeit gegen die Anwendung von Methoden des Social Engineering zu erhöhen.
- mit verschiedenen Interessengruppen wie nationalen Sicherheitsbehörden, Sicherheitsunternehmen und Internetdiensteanbietern zusammenzuarbeiten.

## Kursinhalt

- Dieser Projektkurs konzentriert sich auf praktische Aspekte zur Verhinderung, Aufdeckung und Abwehr von Angriffen, die durch Social Engineering ausgelöst werden, sowie auf die Bedrohung durch feindliche Insider. Die Studierenden beginnen mit einem ausgewählten

Anwendungsfall, um eine greifbare und erfolgreiche Social-Engineering-Kampagne zu analysieren, die Hauptangriffsvektoren zu identifizieren und zu lernen, wie verschiedene Aktivitäten auf mehreren Ebenen zusammenwirken, um das Ziel oder den Angreifer zu erreichen. Die Studierenden müssen den Sicherheitsrahmen des angegriffenen Unternehmens analysieren und die Schwachstellen und Defizite identifizieren, die den Social Engineering-Angriff erfolgreich ermöglichten.

- Unter Berücksichtigung des "menschlichen Faktors" sollen die Studierenden dann organisatorische und technische Sicherheitsrichtlinien entwickeln, um aufzuzeigen, wie ein bestimmter Angriff hätte verhindert und der Schaden vermieden oder gemildert werden können. Alle relevanten Artefakte und Überlegungen werden von den Studierenden in einem umfassenden Projektbericht dokumentiert.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Blokdyk, G. (2019). Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited.
- Company. TrustedSec. (Internet DEMO Version to subscribe)
- Gelles, M. G. (2016). Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann,.
- Hadnagy, C. (2012). Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe, MITP-Verlags GmbH & Co. KG.
- Menger, A. (2016): IT-Sicherheit und Social Engineering. Grundlagen, Erscheinungsformen und Schutzmöglichkeiten. Hochschule Osnabrück
- Michael Bartsch & Stefanie Frey (2018). Cybersecurity Best Practices : Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Fachmedien Wiesbaden.
- Thomas Liedtke (2022). Informationssicherheit: Möglichkeiten und Grenzen. Springer Berlin.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Projektpräsentation

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien



## Host Forensics

Module Code: DLBCSEEHF\_E

<b>Module Type</b> see curriculum	<b>Admission Requirements</b> <ul style="list-style-type: none"> <li>▪ DLBCSEHSF01_E or DLBCSEHSF01_D</li> <li>▪ DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E</li> </ul>	<b>Study Level</b> BA	<b>CP</b> 10	<b>Student Workload</b> 300 h
--------------------------------------	---	--------------------------	-----------------	----------------------------------

<b>Semester / Term</b> see curriculum	<b>Duration</b> Minimum 1 semester	<b>Regularly offered in</b> WiSe/SoSe	<b>Language of Instruction and Examination</b> English
--	--	--	---

### Module Coordinator

N.N. (Static and Dynamic Malware Analysis) / N.N. (Seminar: Sandbox Interpretation)

### Contributing Courses to Module

- Static and Dynamic Malware Analysis (DLBCSEEHF01\_E)
- Seminar: Sandbox Interpretation (DLBCSEEHF02\_E)

### Module Exam Type

#### Module Exam

#### Split Exam

Static and Dynamic Malware Analysis

- Study Format "Distance Learning": Exam, 90 Minutes

Seminar: Sandbox Interpretation

- Study Format "Distance Learning": Written Assessment: Research Essay

### Weight of Module

see curriculum

**Module Contents****Static and Dynamic Malware Analysis**

- Objectives in Malware analysis
- Analysis Lab setup
- Tools of the trade
- Malware Classification
- Sandboxes
- Reversing
- Digging deeper

**Seminar: Sandbox Interpretation**

This course is about the practical application of Malware analysis techniques to real sandbox log files.

**Learning Outcomes****Static and Dynamic Malware Analysis**

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

**Seminar: Sandbox Interpretation**

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

**Links to other Modules within the Study Program**

This module is similar to other modules in the fields of Computer Science & Software Development

**Links to other Study Programs of the University**

All Bachelor Programs in the IT & Technology fields

## Static and Dynamic Malware Analysis

Course Code: DLBCSEEHF01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D

### Course Description

Malware is a top compromise vector in cyber attacks. Analyzing the attacking Malware gives the security analyst insights into the methodology and intension of the attacker. There are a number of ways that Malware can be analyzed and this course will introduce the most common ones.

### Course Outcomes

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

### Contents

1. Objectives in Malware analysis
  - 1.1 Forensics
  - 1.2 Root cause analysis
  - 1.3 Mitigation
2. Analysis Lab setup
  - 2.1 Stealth
  - 2.2 Isolation
  - 2.3 Honeypots
3. Tools of the trade
  - 3.1 Virtual machines
  - 3.2 Debugger
  - 3.3 Disassembler

4. Malware Classification
  - 4.1 Antivirus
  - 4.2 Virustotal
  - 4.3 Yara
  - 4.4 Clustering with PEID, TELFHASH, TLSH, SSDEEP, etc
5. Sandboxes
  - 5.1 Levels of interaction
  - 5.2 Instrumentation
  - 5.3 Online sandboxing services, Virustotal
  - 5.4 Scripting for sandboxes
  - 5.5 Corporate sandbox considerations
6. Reversing
  - 6.1 Unpacking, decrypting and de-obfuscation
  - 6.2 Debugging techniques
  - 6.3 Control flow analysis
  - 6.4 Library and system calls
7. Digging deeper
  - 7.1 Domain and IP information
  - 7.2 Analysis of Javascript code
  - 7.3 Memory forensics
  - 7.4 Kernel debugging rootkits
  - 7.5 Theoretical underpinnings of program analysis

**Literature****Compulsory Reading****Further Reading**

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing, Cham.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: <https://beginners.re/> (last accessed: 24 August 2020)

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides

## Seminar: Sandbox Interpretation

Course Code: DLBCSEEHF02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E

### Course Description

In this course, we explore the most important tool in Malware analysis, the Sandbox and extract from the Sandbox logs the potential attacks exhibited by the Malware.

### Course Outcomes

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

### Contents

- This course is about the practical application of Malware analysis techniques to real sandbox log files and extract the indicators of compromise and Malware objectives into a report.

### Literature

#### Compulsory Reading

#### Further Reading

- Gregg, M. (2008): Build Your Own Security Lab: A Field Guide for Network Testing. Wiley, Hoboken, NJ.
- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Seminar
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Research Essay

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides

DLBCSEEHF02\_E



# DevSecOps

Modulcode: DLBCSEEDSO\_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	<ul style="list-style-type: none"> <li>▪ IWNF01 oder IWNF01_E</li> <li>▪ keine</li> </ul>	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

Prof. Dr. Markus Kleffmann (Techniken und Methoden der agilen Softwareentwicklung) /  
N.N. (Projekt: Agiles DevSecOps-Software-Engineering)

## Kurse im Modul

- Techniken und Methoden der agilen Softwareentwicklung (IWNF01)
- Projekt: Agiles DevSecOps-Software-Engineering (DLBCSEEDSO01\_D)

## Art der Prüfung(en)

### Modulprüfung

### Teilmodulprüfung

Techniken und Methoden der agilen Softwareentwicklung

- Studienformat "myStudium": *Prüfungsart*
- Studienformat "Fernstudium": Klausur, 90 Minuten
- Studienformat "Kombistudium": *Prüfungsart*

Projekt: Agiles DevSecOps-Software-Engineering

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****Techniken und Methoden der agilen Softwareentwicklung**

- Merkmale und Prinzipien von Agilität
- Agilität in kleinen Teams mit Scrum
- Agiles Portfolio- und Projektmanagement
- Agiles Anforderungs- und IT-Architekturmanagement
- Agiles Testen
- Agile Delivery and Deployment

**Projekt: Agiles DevSecOps-Software-Engineering**

Dieses Modul behandelt die grundlegenden Sicherheitsprinzipien für die Nutzung von DevOps in der Softwareentwicklung, auch bekannt als das DevSecOps-Paradigma. Anhand eines sicherheitsrelevanten Szenarios werden in diesem Modul gute DevSecOps-Praktiken wie die Definition von Sicherheitsgrundsätzen, Vorgehensweise zur Bedrohungsmodellierung und der Automatisierung von IT-Sicherheitsprozessen als Teil der Continuous Integration/Continuous Development (CI/CD)-Pipeline veranschaulicht.

**Qualifikationsziele des Moduls****Techniken und Methoden der agilen Softwareentwicklung**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Probleme und Risiken der industriellen SW-Entwicklung und ihre Konsequenzen für Entwicklungsprozesse zu analysieren und zu beurteilen.
- die Grundprinzipien des „No-Frills Software Engineering“ zu erläutern.
- Praxisszenarien zu analysieren und selbständig geeignete Methoden und Werkzeuge des „No-Frills Software Engineering“ anzuwenden.

**Projekt: Agiles DevSecOps-Software-Engineering**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Thread-Modellierung in DevOps-Szenarien anzuwenden.
- sich mit den relevanten Sicherheitsgrundsätzen von DevOps aus internationalen Standards und bewährten Praktiken der Industrie vertraut zu machen.
- die geeigneten Werkzeuge und Automatisierungsansätze für DevSecOps auszuwählen.
- die kontinuierliche Überwachung der Einhaltung in „Infrastructure-as-a-Code“ -Szenarien zu entwerfen.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Techniken und Methoden der agilen Softwareentwicklung

Kurscode: IWNF01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen vertiefenden Einblick in das Thema agile Softwareentwicklung zu vermitteln. Dazu werden zunächst die grundlegenden Merkmale und Prinzipien von Agilität vorgestellt und diskutiert. Danach wird dargestellt, wie kleine Projekt und Teams agiles Software-Engineering betreiben können und wie sich die agilen Prinzipien auf große Projekte übertragen und dort anwenden lassen. Anschließend werden agile Techniken für ausgewählte Kernaktivitäten im Software-Engineering vermittelt, wobei ein Schwerpunkt auf dem Gebiet Testen, Delivery und Deployment liegt.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Probleme und Risiken der industriellen SW-Entwicklung und ihre Konsequenzen für Entwicklungsprozesse zu analysieren und zu beurteilen.
- die Grundprinzipien des „No-Frills Software Engineering“ zu erläutern.
- Praxisszenarien zu analysieren und selbständig geeignete Methoden und Werkzeuge des „No-Frills Software Engineering“ anzuwenden.

## Kursinhalt

1. Merkmale und Prinzipien von Agilität
  - 1.1 Merkmale und Herausforderungen von Softwareprojekten
  - 1.2 Klassifikation von Unsicherheit
  - 1.3 Gegenüberstellung von agiler und klassischer Softwareentwicklung
  - 1.4 Prinzipien von Agilität
2. Agilität in kleinen Teams mit Scrum
  - 2.1 Grundlagen und allgemeiner Aufbau mit Scrum
  - 2.2 Zentrales Managementartefakt: Product Backlog
  - 2.3 Weitere Managementartefakte

3. Agiles Portfolio- und Projektmanagement
  - 3.1 Planungsebenen im agilen Projektmanagement
  - 3.2 Agiles Portfoliomanagement
  - 3.3 Organisation mehrerer Teams in einem Projekt
  - 3.4 Produkt- und Release-Planung
4. Agiles Anforderungs- und IT-Architekturmanagement
  - 4.1 Requirements Engineering in agilen Projekten
  - 4.2 Architekturmanagement in agilen Projekten
5. Agiles Testen
  - 5.1 Grundlagen und Anforderungen an die QS-Organisation
  - 5.2 Teststufen und Agilität
  - 5.3 Testautomatisierung
6. Agile Delivery and Deployment
  - 6.1 Grundlagen und Continuous Delivery Pipeline
  - 6.2 Continuous Build and Continuous Integration
  - 6.3 Akzeptanztests, Lasttests und Continuous Deployment

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Baumgartner, M. et al. (2013): Agile Testing. Der agile Weg zur Qualität. Hanser, München.
- Biffel, S. et al. (Hrsg.) (2005): Value-Based Software Engineering. Springer, Berlin/Heidelberg.
- Cockburn, A. (2007): Agile Software Development. The Cooperative Game. 2. Auflage, Addison-Wesley, Upper Saddle River (NJ).
- DeMarco, T. (2003): Bärenango. Mit Risikomanagement Projekte zum Erfolg führen. Hanser, München.
- Epping, T. (2011): Kanban für die Softwareentwicklung. Springer, Berlin/Heidelberg.
- Geirhos, M. (2011): IT-Projektmanagement. Was wirklich funktioniert – und was nicht. Galileo Computing, Bonn.
- Hummel, H. (2011): Aufwandsschätzungen in der Software- und Systementwicklung. Spektrum, Wiesbaden.
- Künneth, T. (2012): Android 4. Apps entwickeln mit dem Android SDK. Galileo Computing, Bonn.
- Link, J. (2005): Softwaretests mit JUnit. 2.Auflage, dpunkt.verlag, Heidelberg.
- Mangold, P. (2009): IT-Projektmanagement. 3. Auflage, Spektrum, Wiesbaden.
- Motzel, E./O. Pannenbäcker (1998): Projektmanagement-Kanon. Der deutsche Zugang zum Project Management Body of Knowledge. TÜV-Verlag, Köln.
- Pichler, R. (2007): Scrum. Agiles Projektmanagement erfolgreich einsetzen. dpunkt.verlag, Heidelberg. (2007)
- Röpstorff, S./Wiechmann, R. (2012): Scrum in der Praxis. Erfahrungen, Problemfelder und Erfolgsfaktoren. dpunkt.verlag, Heidelberg.
- Rubin, K. S. (2014): Essential Scrum. Umfassendes Scrum-Wissen aus der Praxis. mitp, Frechen.
- Tiemeyer, E. (2010): Handbuch IT-Projektmanagement, Vorgehensmodelle, Managementinstrumente, Good Practices. Hanser, München.
- Wirdemann, R. (2011): Scrum mit User Stories. 2. Auflage, Hanser, München.
- Wolff, E. (2014): Continuous Delivery. Der pragmatische Einstieg. dpunkt.verlag, Heidelberg.
- Wolf, H./Bleek/W.-G. (2010): Agile Softwareentwicklung. Werte, Konzepte und Methoden. 2. Auflage, dpunkt.verlag, Heidelberg.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b>
---------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b>
------------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien



# Projekt: Agiles DevSecOps-Software-Engineering

Kurscode: DLBCSEEDSO01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IWNF01 oder IWNF01_E

## Beschreibung des Kurses

Trotz der breiten Akzeptanz von DevOps in der Industrie ist die Integration von Sicherheitsprinzipien in dieses Paradigma (d.h. DevSecOps) für e viele IT-Fachleute immer noch eine große Herausforderung. In diesem Kurs lernen die KursteilnehmerInnen grundlegende DevSecOps-Konzepte kennen, wie z.B. die Modellierung von Bedrohungen, die Definition von Sicherheitsgrundsätzen, die kontinuierliche Überwachung der Einhaltung und die Integration der Automatisierung von IT-Sicherheitsprozessen in DevOps.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Thread-Modellierung in DevOps-Szenarien anzuwenden.
- sich mit den relevanten Sicherheitsgrundsätzen von DevOps aus internationalen Standards und bewährten Praktiken der Industrie vertraut zu machen.
- die geeigneten Werkzeuge und Automatisierungsansätze für DevSecOps auszuwählen.
- die kontinuierliche Überwachung der Einhaltung in „Infrastructure-as-a-Code“ -Szenarien zu entwerfen.

## Kursinhalt

- Dieser Kurs behandelt die grundlegenden Sicherheitsprinzipien zur Nutzung des DevSecOps-Ansatzes in Softwaretechnologie Szenarien. Der Inhalt dieses Kurses veranschaulicht die Anwendung von DevSecOps, um die Sicherheit einer Organisation kontinuierlich und ganzheitlich zu verbessern, anstatt sich nur auf den Schutz der zugrundeliegenden Software-Infrastruktur zu konzentrieren (wie im Fall traditioneller, nicht-agiler Methoden). Durch die Präsentation von DevSecOps-Prinzipien wie Bedrohungsmodellierung, Definition von Sicherheitsgrundsätzen, Werkzeuge der Automatisierung von IT-Sicherheitsprozessen und kontinuierliche Überwachung der Einhaltung von Vorschriften wird dieser Kurs vermitteln, wie Sicherheit bei der Entwicklung eines Softwaretechnologie Produkts integriert werden kann.

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Johnson, E. (2020): Secure DevOps. A Practical Introduction. (URL: <https://www.sans.org/ondemand/course/secure-dev-ops-a-practical-introduction> [Retrieved: 15.08.2020]).
- Hsu, T. (2018): Hands-On Security in DevOps. Packt Publishing, UK.
- Microsoft. (2020): Secure DevOps. Making security principles and practices an integral part of DevOps while maintaining improved efficiency and productivity. (URL: <https://www.microsoft.com/en-us/securityengineering/devsecops> [Retrieved: 15.08.2020]).
- Schneider, C. (2015): Security DevOps. Staying secure in agile projects. (URL: <https://owaspappseceurope2015.sched.com/event/378l/security-devops-staying-secure-in-agile-projects> [Retrieved: 15.08.2020]).
- Yasar, H. (2016): An Introduction to Secure DevOps. Including Security in the Software Lifecycle. (URL: <https://insights.sei.cmu.edu/devops/2016/11/an-introduction-to-secure-devops-including-security-in-the-software-lifecycle.html> [Retrieved: 15.08.2020]).

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input checked="" type="checkbox"/> Folien
<input type="checkbox"/> Musterklausur	

DLBCSEEDS001\_D

## Sicherheit in komplexen Netzwerken

Modulcode: DLBCSEESCN\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ IAMG01 oder DLBCSEITPAM02</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	--	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof.Dr. Holger Klus (IT-Architekturmanagement) / N.N. (Projekt: IT-Sicherheitsarchitekturen)

### Kurse im Modul

- IT-Architekturmanagement (IAMG01)
- Projekt: IT-Sicherheitsarchitekturen (DLBCSEESCN01\_D)

### Art der Prüfung(en)

<b>Modulprüfung</b>	<b>Teilmodulprüfung</b>
	<u>IT-Architekturmanagement</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> <li>• Studienformat "Kombistudium": Klausur</li> </ul> <u>Projekt: IT-Sicherheitsarchitekturen</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****IT-Architekturmanagement**

- Grundlagen und Begriffe zum Management von IT-Unternehmensarchitekturen
- IT-Anwendungsportfoliomanagement
- Architektur-Governance
- Modellierung von IT-Unternehmensarchitekturen
- Frameworks am Beispiel von TOGAF
- Referenzmodelle und Musterkataloge

**Projekt: IT-Sicherheitsarchitekturen**

Umsetzung und Dokumentation praktischer Fragen zur IT-Sicherheit im Rahmen des IT-Architekturmanagements.

**Qualifikationsziele des Moduls****IT-Architekturmanagement**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundprinzipien von IT-Strategie, IT-Governance und IT-Architekturmanagement zu kennen, diese zu erläutern und voneinander abzugrenzen.
- die typischen Aktivitäten des IT-Architekturmanagements, deren Zusammenhänge und deren Abhängigkeiten zu erläutern und voneinander abzugrenzen.
- geeignete Modelle des IT-Architekturmanagements zu erkennen, sie voneinander abzugrenzen und deren Verwendungszweck zu erläutern.
- die Elemente und Inhalte ausgewählter IT-Architekturframeworks sowie Referenzmodelle und Musterkataloge zu erkennen.

**Projekt: IT-Sicherheitsarchitekturen**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-Architektur-Management-Tools und -Techniken aus der Perspektive der IT-Sicherheit einzusetzen.
- eine IT-Architektur im Hinblick auf IT-Sicherheitslücken eigenständig zu analysieren.
- eine IT-Sicherheitsarchitektur zu entwerfen und sie in das gesamte IT-Architekturmanagement zu integrieren.
- Probleme im Spannungsfeld zwischen betrieblichen, finanziellen und Management-Bedürfnissen und IT-Sicherheitsanforderungen zu identifizieren und zu erklären.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# IT-Architekturmanagement

Kurscode: IAMG01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Neben konkreten IT-Projekten, z. B. die Neuentwicklung eines IT-Systems oder die Einführung einer Standardsoftware, muss für die organisationsweite IT-Infrastruktur – also die Menge aller eingesetzter IT-Hardware und -Softwaresysteme – ein strategisches Management eingesetzt werden. Diese Leitung obliegt dem IT-Unternehmensarchitekten, der das IT-Architekturmanagement betreibt. Seine Aufgabe ist die strategische Ausrichtung der IT-Infrastruktur an die Geschäfts- und IT-Strategie der Organisation. Dieser Kurs vermittelt typische Konzepte, Methoden, Vorgehensweisen und Modelle für die Aufgaben im Rahmen des IT-Architekturmanagements.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundprinzipien von IT-Strategie, IT-Governance und IT-Architekturmanagement zu kennen, diese zu erläutern und voneinander abzugrenzen.
- die typischen Aktivitäten des IT-Architekturmanagements, deren Zusammenhänge und deren Abhängigkeiten zu erläutern und voneinander abzugrenzen.
- geeignete Modelle des IT-Architekturmanagements zu erkennen, sie voneinander abzugrenzen und deren Verwendungszweck zu erläutern.
- die Elemente und Inhalte ausgewählter IT-Architekturframeworks sowie Referenzmodelle und Musterkataloge zu erkennen.

## Kursinhalt

1. Grundlagen und Begriffe zum Management von IT-Unternehmensarchitekturen
  - 1.1 IT-Unternehmensarchitektur
  - 1.2 Ziele von Enterprise Architecture Management
  - 1.3 Prozesse im Management von IT-Unternehmensarchitekturen
2. IT-Anwendungsportfoliomanagement
  - 2.1 Überblick über das IT-Anwendungsportfoliomanagement
  - 2.2 Anwendungshandbuch
  - 2.3 Portfolioanalyse
  - 2.4 Bebauungsplanung

3. Architektur-Governance
  - 3.1 Aufbauorganisation
  - 3.2 Entwicklung und Durchsetzung von Richtlinien
  - 3.3 Projektbegleitung
4. Modellierung von IT-Unternehmensarchitekturen
  - 4.1 Modelle im Kontext IT-Architekturmanagement
  - 4.2 Dokumentationsformen für Prozesse und Anwendungen
  - 4.3 Dokumentationsformen für Systeme und Technologien
5. Frameworks am Beispiel von TOGAF
  - 5.1 Grundlagen und Einsatz von IT-Architekturframeworks
  - 5.2 Überblick und Kategorien von EAM-Frameworks
  - 5.3 The Open Group Architecture Framework (TOGAF)
6. Referenzmodelle und Musterkataloge
  - 6.1 Referenzmodelle für Architekturen
  - 6.2 Musterkatalog für Gestaltung von EAM

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Hanschke, I. (2011): Enterprise Architecture Management. Einfach und effektiv. Hanser, München.
- Keller, W. (2012): IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung. 2. Auflage, dpunkt.verlag, Heidelberg.
- Keuntje, J. H./Barkow, R. (Hrsg.) (2010): Enterprise Architecture. Management in der Praxis. Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen.
- Ross, J. W./ Weill, P./Robertson, D. C. (2006): Enterprise Architecture as Strategy. Creating a Foundation for Business Execution. Harvard Business Review Press, Boston.
- Schwarzer, B. (2009): Einführung in das Enterprise Architecture Management. Verstehen – Planen – Umsetzen. Books on Demand, Norderstedt.



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien

## Projekt: IT-Sicherheitsarchitekturen

Kurscode: DLBCSEESC01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IAMG01 oder DLBCSEITPAM02

### Beschreibung des Kurses

Unter Verwendung von Methoden und Techniken aus dem Bereich IT-Architekturmanagement bearbeiten die Studierenden in diesem Kurs selbständig eine praktische Fragestellung im Bereich der IT-Sicherheitsarchitektur. Am Ende des Kurses sind die Studierenden in der Lage, auf der Basis einer bestehenden IT-System- / Netzwerkarchitektur eine IT-Sicherheitsarchitektur selbstständig zu entwickeln.

### Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-Architektur-Management-Tools und -Techniken aus der Perspektive der IT-Sicherheit einzusetzen.
- eine IT-Architektur im Hinblick auf IT-Sicherheitslücken eigenständig zu analysieren.
- eine IT-Sicherheitsarchitektur zu entwerfen und sie in das gesamte IT-Architekturmanagement zu integrieren.
- Probleme im Spannungsfeld zwischen betrieblichen, finanziellen und Management-Bedürfnissen und IT-Sicherheitsanforderungen zu identifizieren und zu erklären.

### Kursinhalt

- Umsetzung und Dokumentation praktischer Fragen zur IT-Sicherheit im Rahmen des IT-Architekturmanagements. Typische Szenarien sind z.B. "Implementierung von IT-Sicherheitsgeräten in komplexen Netzwerken", "Gestaltung von Prozessen für Sicherheitsupdates und Patch-Management" und "Einsatz von Inhouse-Ressourcen oder Outsourcing von IT-Sicherheitsaufgaben".

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Bartsch, M. / Frey, S. (2014): Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Fachmedien, Wiesbaden.
- Müller, K.-R. (2014): IT-Sicherheit mit System. 5. Auflage, Springer Fachmedien, Wiesbaden.
- Pfister, M. (2019): Info Guard Swiss Cyber Security - In 3 einfachen (aber wichtigen) Schritten zur Enterprise IT-Sicherheitsarchitektur. (URL: [www.infoguard.ch](http://www.infoguard.ch) [zuletzt besucht am 22.08.2020]).

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

DLBCSEESCNO1\_D

## Network Forensics

Module Code: DLBCSEENF\_E

<b>Module Type</b> see curriculum	<b>Admission Requirements</b> <ul style="list-style-type: none"> <li>▪ DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E</li> <li>▪ DLBCSEINF01_E or DLBCSEINF01_D</li> </ul>	<b>Study Level</b> BA	<b>CP</b> 10	<b>Student Workload</b> 300 h
--------------------------------------	---	--------------------------	-----------------	----------------------------------

<b>Semester / Term</b> see curriculum	<b>Duration</b> Minimum 1 semester	<b>Regularly offered in</b> WiSe/SoSe	<b>Language of Instruction and Examination</b> English
--	--	--	---

### Module Coordinator

Dr. Rachel John Robinson (Protocols, Log- and Dataflow-Analysis in Depth) / N.N. (Seminar: Threat Hunting, Analysis and Incident Response)

### Contributing Courses to Module

- Protocols, Log- and Dataflow-Analysis in Depth (DLBCSEENF01\_E)
- Seminar: Threat Hunting, Analysis and Incident Response (DLBCSEENF02\_E)

### Module Exam Type

<b>Module Exam</b>	<b>Split Exam</b> <u>Protocols, Log- and Dataflow-Analysis in Depth</u> <ul style="list-style-type: none"> <li>• Study Format "Distance Learning": Exam, 90 Minutes</li> </ul> <u>Seminar: Threat Hunting, Analysis and Incident Response</u> <ul style="list-style-type: none"> <li>• Study Format "Distance Learning": Written Assessment: Research Essay</li> </ul>
--------------------	---

### Weight of Module

see curriculum

<p><b>Module Contents</b></p> <p><b>Protocols, Log- and Dataflow-Analysis in Depth</b></p> <ul style="list-style-type: none"> <li>▪ Network Basics</li> <li>▪ Operating System Logs</li> <li>▪ Packet Capturing and Analysis</li> <li>▪ Log Management</li> <li>▪ Preparation for Attacks</li> <li>▪ Intrusion Detection and Prevention System</li> </ul> <p><b>Seminar: Threat Hunting, Analysis and Incident Response</b></p> <ul style="list-style-type: none"> <li>▪ Mitre ATT&amp;CK TTPs</li> <li>▪ APT actors</li> <li>▪ Security coverage gap analysis</li> </ul>	
<p><b>Learning Outcomes</b></p> <p><b>Protocols, Log- and Dataflow-Analysis in Depth</b></p> <p>On successful completion, students will be able to</p> <ul style="list-style-type: none"> <li>▪ locate and evaluate security relevant log data.</li> <li>▪ operate a typical SIEM system.</li> <li>▪ create and understand SOC procedures.</li> <li>▪ report findings in written and machine readable forms.</li> </ul> <p><b>Seminar: Threat Hunting, Analysis and Incident Response</b></p> <p>On successful completion, students will be able to</p> <ul style="list-style-type: none"> <li>▪ understand Mitre ATT&amp;CK® Techniques, Tactics and Procedures.</li> <li>▪ understand how APT actors use combinations of these TTPs.</li> <li>▪ understand how Botnets and related Malware behave in networks.</li> <li>▪ examine where to find evidence of these TTPs.</li> <li>▪ explore datasets for threats not picked up by existing rules.</li> <li>▪ do a gap analysis on existing protections with respect to a given APT.</li> <li>▪ design mitigations to given TTPs.</li> </ul>	
<p><b>Links to other Modules within the Study Program</b></p> <p>This module is similar to other modules in the fields of Computer Science &amp; Software Development</p>	<p><b>Links to other Study Programs of the University</b></p> <p>All Bachelor Programs in the IT &amp; Technology fields</p>



## Protocols, Log- and Dataflow-Analysis in Depth

Course Code: DLBCSEENF01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D

### Course Description

Logging is done for a variety of diagnosis reasons, but these logs can be very useful in finding security incidents. In this course, we look at a variety of sources of log files. These range from operating system logs, to application logs and network traffic logs. Context and additional information also need to be collected. All this data is then consolidated in a Security Information and Event Management system where it can be analyzed and triaged for action. Finally, major incidents need to be documented and communicated to the relevant parties.

### Course Outcomes

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

### Contents

1. Introduction to Network Forensics
  - 1.1 Basics of Network Forensics
  - 1.2 Evidence Handling Standards
  - 1.3 Verification of Evidence
2. Network Basics
  - 2.1 Protocol Basics and Functionality
  - 2.2 Difference between the OSI Model and TCP/IP Architecture
  - 2.3 Basics of TCP and UDP including Ports and Protocols
  - 2.4 DNS, DHCP and ARP
3. Host-Side Artifacts
  - 3.1 Network-based Artifacts stored in the Operating Systems
  - 3.2 Services and Ports
  - 3.3 TCP Connection States
  - 3.4 Tools for extracting the Artifacts

4. Packet Capture and Analysis
  - 4.1 Capturing Packets
  - 4.2 Tools like TCPDump and Wireshark
  - 4.3 Analysis of captured Packets
5. Location Information
  - 5.1 Impact of Time Zones on Investigations
  - 5.2 Location Information from the Network
  - 5.3 Location-based Services with Web Applications
  - 5.4 Location Information from WiFi
6. Preparing for Attacks
  - 6.1 Manage Netflow Data
  - 6.2 Loggings
  - 6.3 Antivirus
  - 6.4 SIEM and Incident Response
7. Intrusion Detection and Prevention Systems
  - 7.1 Detection Styles
  - 7.2 Host-based versus Network-based
  - 7.3 Challenges with Intrusion Detection and Prevention Systems
  - 7.4 Firewall and Application Logs
8. Correlation of Data
  - 8.1 Synchronization of Time across Multiple Systems
  - 8.2 Log Aggregation and Management
  - 8.3 Importance of Timelines

**Literature****Compulsory Reading****Further Reading**

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- NIST Special Publication 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides

## Seminar: Threat Hunting, Analysis and Incident Response

Course Code: DLBCSEENF02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E

### Course Description

Much of a security officer's work is with data where incidents need to be analyzed and countermeasures implemented. This course uses the Mitre ATT&CK® framework to reference TTPs (Techniques, Tactics and Procedures) that map to security events. Not all TTPs can be found in labeled security events, so Threat Hunting aims to go beyond ordinary incident response and find indicators of these TTPs also using other methods.

### Course Outcomes

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

### Contents

- In this seminar, we cover the subjects of incident response and threat hunting using the Mitre ATT&CK® framework and publicly available reports.

### Literature

#### Compulsory Reading

#### Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Seminar
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Research Essay

<b>Student Workload</b>					
<b>Self Study</b> 120 h	<b>Contact Hours</b> 0 h	<b>Tutorial</b> 30 h	<b>Self Test</b> 0 h	<b>Independent Study</b> 0 h	<b>Hours Total</b> 150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides

DLBCSEENF02\_E







# 6. Semester

---



# Business Intelligence

Modulcode: IWBI

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	--	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

<b>Modulverantwortliche(r)</b> Dr. Peter Poensgen (Business Intelligence ) / Dr. Peter Poensgen (Projekt Business Intelligence)
--

<b>Kurse im Modul</b>
<ul style="list-style-type: none"> <li>▪ Business Intelligence (IWBI01)</li> <li>▪ Projekt Business Intelligence (IWBI02)</li> </ul>

<b>Art der Prüfung(en)</b>						
<b>Modulprüfung</b>	<table border="0"> <tr> <td><b>Teilmodulprüfung</b></td> </tr> <tr> <td><u>Business Intelligence</u></td> </tr> <tr> <td> <ul style="list-style-type: none"> <li>• Studienformat "myStudium": Klausur, 90 Minuten</li> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> <li>• Studienformat "Kombistudium": Klausur, 90 Minuten</li> </ul> </td> </tr> <tr> <td><u>Projekt Business Intelligence</u></td> </tr> <tr> <td> <ul style="list-style-type: none"> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul> </td> </tr> </table>	<b>Teilmodulprüfung</b>	<u>Business Intelligence</u>	<ul style="list-style-type: none"> <li>• Studienformat "myStudium": Klausur, 90 Minuten</li> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> <li>• Studienformat "Kombistudium": Klausur, 90 Minuten</li> </ul>	<u>Projekt Business Intelligence</u>	<ul style="list-style-type: none"> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>
<b>Teilmodulprüfung</b>						
<u>Business Intelligence</u>						
<ul style="list-style-type: none"> <li>• Studienformat "myStudium": Klausur, 90 Minuten</li> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> <li>• Studienformat "Kombistudium": Klausur, 90 Minuten</li> </ul>						
<u>Projekt Business Intelligence</u>						
<ul style="list-style-type: none"> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>						

**Anteil der Modulnote an der Gesamtnote**

s. Curriculum

**Lehrinhalt des Moduls****Business Intelligence**

- Motivation und Begriffsbildung
- Datenbereitstellung
- Data Warehouse
- Modellierung multidimensionaler Datenräume
- Analysesysteme
- Distribution und Zugriff

**Projekt Business Intelligence**

Mögliche Themengebiete für das BI-Projekt sind u.a. „Management von BI-Projekten, „Konzeption von multidimensionalen Datenmodellen“ sowie „Prototypische Umsetzung von kleinen BI-Anwendungen“.

**Qualifikationsziele des Moduls****Business Intelligence**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivation, Anwendungsfälle und Grundlagen für Business Intelligence zu erklären.
- Techniken und Methoden zur Bereitstellung und Modellierung von Daten sowie für BI relevante Arten von Daten zu benennen und zu erläutern sowie voneinander abzugrenzen.
- Techniken und Methoden zur Informationsgenerierung und -speicherung zu erläutern und auf Basis konkreter Anforderungen selbstständig geeignete Methoden auszuwählen.

**Projekt Business Intelligence**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine Lösung zu einer praktischen Fragestellung im Thema Business Intelligence zu konzipieren, prototypisch umzusetzen und die dabei erzielten Ergebnisse zu dokumentieren.
- typische Probleme und Herausforderungen in der Konzeption und praktischen Umsetzung kleiner BI-Lösungen zu benennen und zu erläutern.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Business Intelligence

Kurscode: IWBI01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Business Intelligence (BI) dient der Gewinnung von Informationen aus Unternehmensdaten, die sowohl für eine gezielte Unternehmenssteuerung als auch für die Optimierung von Geschäftsaktivitäten relevant sind. Im Rahmen dieses Kurses werden Techniken, Vorgehensweisen und Modelle zur Datenbereitstellung, Informationsgenerierung und -analyse sowie der Verteilung der gewonnenen Informationen vorgestellt und diskutiert. Sie werden danach in der Lage sein, die verschiedenen Themengebiete des Data Warehousing zu erläutern und Methoden bzw. Techniken für konkrete Anforderungen selbstständig auszuwählen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivation, Anwendungsfälle und Grundlagen für Business Intelligence zu erklären.
- Techniken und Methoden zur Bereitstellung und Modellierung von Daten sowie für BI relevante Arten von Daten zu benennen und zu erläutern sowie voneinander abzugrenzen.
- Techniken und Methoden zur Informationsgenerierung und -speicherung zu erläutern und auf Basis konkreter Anforderungen selbstständig geeignete Methoden auszuwählen.

## Kursinhalt

1. Motivation und Begriffsbildung
  - 1.1 Motivation und historische Entwicklung
  - 1.2 BI als Rahmenwerk
2. Datenbereitstellung
  - 2.1 Operative und dispositive Systeme
  - 2.2 Das Data-Warehouse-Konzept
  - 2.3 Architekturvarianten
3. Data Warehouse
  - 3.1 ETL-Prozess
  - 3.2 DWH und Data Mart
  - 3.3 ODS und Metadaten

4. Modellierung multidimensionaler Datenräume

- 4.1 Datenmodellierung
- 4.2 OLAP-Würfel
- 4.3 Physische Speicherung
- 4.4 Star- und Snowflake-Schema
- 4.5 Historisierung

5. Analysensysteme

- 5.1 Freie Datenrecherche und OLAP
- 5.2 Berichtssysteme
- 5.3 Modellgestützte Analysensysteme
- 5.4 Konzeptorientierte Systeme

6. Distribution und Zugriff

- 6.1 Informationsdistribution
- 6.2 Informationszugriff

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Bachmann, R./Kemper, G. (2011): Raus aus der BI-Falle. Wie Business Intelligence zum Erfolg wird. 2. Auflage, mitp, Heidelberg.
- Bauer, A./Günzel, H. (2008): Data Warehouse Systeme. Architektur, Entwicklung, Anwendung. 3. Auflage, dpunkt.verlag, Heidelberg.
- Betz, R. (2015): Werde Jäger des verlorenen Schatzes. In: Immobilienwirtschaft, Heft 5, S. 1614–1164. (URL <https://www.haufe.de/download/immobilienwirtschaft-ausgabe-052015-immobilienwirtschaft-fachmagazin-fuer-management-recht-praxis-303530.pdf> [letzter Zugriff: 27.02.2017]).
- Bodendorf, F. (2006): Daten- und Wissensmanagement. 2. Auflage, Springer, Berlin.
- Chamoni, P./Gluchowski, P. (Hrsg.) (2006): Analytische Informationssysteme Business Intelligence-Technologien und -Anwendungen. Springer, Berlin.
- Engels, C. (2008): Basiswissen Business Intelligence. W3L, Herdecke/Witten.
- Gansor, T./Totok, A./Stock, S. (2010): Von der Strategie zum Business Intelligence Competency Center (BICC). Konzeption – Betrieb – Praxis. Hanser, München.
- Gluchowski, P./Gabriel, R./Dittmar, C. (2008): Management Support Systeme und Business Intelligence. Computergestützte Informationssysteme für Fach- und Führungskräfte. 2. Auflage, Springer, Berlin/Heidelberg.
- Grothe, M. (2000): Business Intelligence. Aus Informationen Wettbewerbsvorteile gewinnen. Addison-Wesley, München.
- Gutenberg, E. (1983): Grundlagen der Betriebswirtschaft, Band 1. Die Produktion. 18. Auflage, Springer, Berlin/Heidelberg/New York.
- Hannig, U. (Hrsg.) (2002): Knowledge Management und Business Intelligence. Springer, Berlin.
- Hansen, H.-R./Neumann, G. (2001): Wirtschaftsinformatik I. Grundlagen betrieblicher Informationsverarbeitung. 8. Auflage, Lucius & Lucius UTB, Stuttgart.
- Humm, B./Wietek, F. (2005): Architektur von Data Warehouses und Business Intelligence Systemen. In: Informatik Spektrum, S. 3–14. (URL: [https://www.fbi.h-da.de/fileadmin/personal/b.humm/Publikationen/Humm\\_\\_Wietek\\_-\\_Architektur\\_DW\\_\\_Informatik-Spektrum\\_2005-01\\_.pdf](https://www.fbi.h-da.de/fileadmin/personal/b.humm/Publikationen/Humm__Wietek_-_Architektur_DW__Informatik-Spektrum_2005-01_.pdf) [letzter Zugriff: 27.02.2017]).
- Kemper, H.-G./Baars, H./Mehanna, W. (2010): Business Intelligence – Grundlagen und praktische Anwendungen. Eine Einführung in die IT-basierte Managementunterstützung. 3. Auflage, Vieweg+Teubner, Stuttgart.
- Turban, E. et al. (2010): Business Intelligence. A Managerial Approach. 2. Auflage, Prentice Hall, Upper Saddle River (NJ).

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# Projekt Business Intelligence

Kurscode: IWB102

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Unter Anwendung bekannter Methoden und Techniken aus dem Themengebiet Business Intelligence bearbeiten die Studierenden in diesem Kurs selbstständig eine praktische Fragestellung. Zum Abschluss des Kurses können Sie selbstständig auf der Grundlage konkreter Anforderungen Business Intelligence-Anwendungen konzipieren und prototypisch umsetzen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine Lösung zu einer praktischen Fragestellung im Thema Business Intelligence zu konzipieren, prototypisch umzusetzen und die dabei erzielten Ergebnisse zu dokumentieren.
- typische Probleme und Herausforderungen in der Konzeption und praktischen Umsetzung kleiner BI-Lösungen zu benennen und zu erläutern.

## Kursinhalt

- Umsetzung und Dokumentation von praktischen Fragestellungen zum Einsatz von Business Intelligence-Anwendungen. Typische Szenarien sind beispielsweise „Management von BI-Projekten“, „Konzeption von multidimensionalen Datenmodellen“ und „Prototypische Umsetzung von kleinen BI-Anwendungen“.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Brenner, W./Uebernicketel, F. (2015): Design Thinking. Das Handbuch. Frankfurter Allgemeine Buch, Frankfurt a. M.
- Brown, T. (2008): Design Thinking. In: Harvard Business Review, Heft Juni, S. 84–95.
- Meinel, C./Weinberg, U./Krohn, T. (Hrsg.) (2015): Design Thinking Live. Wie man Ideen entwickelt und Probleme löst. Murmann, Hamburg.
- Uebernicketel, F./Brenner, W. (2016): Design Thinking. In: Hoffmann, C. P. et al. (Hrsg.): Business Innovation: Das St. Galler Modell. Springer, Wiesbaden, S. 243–265.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Projekt
------------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Projekt
---------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

## Future Threats

Modulcode: DLBCSEEF\_T\_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	<ul style="list-style-type: none"> <li>▪ IREN01 oder DLBCSRE01; DLBCSEEF_T01_D oder DLBCSEEF_T01_E</li> <li>▪ IREN01 oder DLBCSRE01</li> </ul>	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

### Modulverantwortliche(r)

N.N. (Threat Modeling) / N.N. (Projekt: Threat Modeling)

### Kurse im Modul

- Threat Modeling (DLBCSEEF\_T01\_D)
- Projekt: Threat Modeling (DLBCSEEF\_T02\_D)

### Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	<u>Threat Modeling</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> </ul> <u>Projekt: Threat Modeling</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>
<b>Anteil der Modulnote an der Gesamtnote</b> s. Curriculum	

**Lehrinhalt des Moduls****Threat Modeling**

- C.I.A. Denken und mehr
- Messung der Cyber-Bedrohung
- Modellierung von Bedrohungen
- Bibliotheken angreifen
- Regeln, Vorschriften und Strafverfolgung
- Risiko-Management
- Threat Mitigation

**Projekt: Threat Modeling**

Dieser Kurs behandelt die Theorie und Praxis des Auffindens und der Modellierung von Bedrohungen in einem bestimmten System, einer bestimmten Architektur oder einem bestimmten Szenario. Er behandelt Methoden und Quellen für übliche Bedrohungsmuster. In einem Projekt wird die Theorie in die Praxis umgesetzt, indem eine gegebene Situation auf Bedrohungen analysiert wird.

**Qualifikationsziele des Moduls****Threat Modeling**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- souverän mögliche Bedrohungsarten zu durchdenken.
- diese Bedrohungen mit Hilfe einer gebräuchlichen Modellierungsmethode zu modellieren.
- relevante Techniken, Taktiken und Verfahren in Bezug auf ein bestimmtes Szenario zu finden.
- das aus dem Bedrohungsmodell hervorgehende Risiko zu ermitteln.
- das Risiko durch die Implementierung von Änderungen des Designs zu mindern.

**Projekt: Threat Modeling**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihr Wissen über die Modellierung von Bedrohungen auf Fälle und Szenarien anzuwenden.
- ihr daraus resultierendes Modell auf der Grundlage einer soliden Argumentation und in Bezug auf bekannte Techniken, Taktiken und Verfahren der Angreifer zu rechtfertigen.
- einen Bericht zu verfassen, der ihre Argumentation in systematischer und verständlicher Weise darlegt.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik



# Threat Modeling

Kurscode: DLBCSEEF01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01

## Beschreibung des Kurses

Wenn ein System oder eine Architektur geschaffen wird, ist es wichtig, dass mögliche Bedrohungen gleichzeitig bewertet werden. Durch die Verwendung sowohl von Modellierungsmethoden als auch von in der Vergangenheit beobachteten Angriffsmustern ist es möglich, ein neues oder bestehendes System auf Bedrohungen hin zu untersuchen. Aus dieser Analyse lassen sich Risiken und Maßnahmen zu deren Verminderung ableiten. Während die gebräuchlichsten Methoden auf den Angriffsbäumen und dem STRIDE-Modell basieren, werden bei der Angriffsmodellierung in letzter Zeit auch Repositorien von Angreifer-Techniken, -Taktiken und -Verfahren (TTP's) zur Inspiration herangezogen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- souverän mögliche Bedrohungsarten zu durchdenken.
- diese Bedrohungen mit Hilfe einer gebräuchlichen Modellierungsmethode zu modellieren.
- relevante Techniken, Taktiken und Verfahren in Bezug auf ein bestimmtes Szenario zu finden.
- das aus dem Bedrohungsmodell hervorgehende Risiko zu ermitteln.
- das Risiko durch die Implementierung von Änderungen des Designs zu mindern.

## Kursinhalt

1. C.I.A. Denken und mehr
  - 1.1 Vertraulichkeit (Confidentiality)
  - 1.2 Integrität (Integrity)
  - 1.3 Verfügbarkeit (Availability)
  - 1.4 Sicherheit und andere Belange
2. Messung der Cyber-Bedrohung
  - 2.1 Messung und Verwaltung
  - 2.2 Metriken zur Cyber-Bedrohung
  - 2.3 Messung der Bedrohung für eine Organisation
  - 2.4 Die Wahrscheinlichkeit größerer Cyber-Angriffe
  - 2.5 Black Swan events

3. Modellierung von Bedrohungen
  - 3.1 Methodik des Angriffsbaumes
  - 3.2 STRIDE
  - 3.3 DREAD
  - 3.4 Schmerzpyramide – “Pyramid of Pain”
4. Bibliotheken angreifen
  - 4.1 CAPEC
  - 4.2 Soloves Taxonomie der Privatsphäre
  - 4.3 Modellierung mit Mitre ATT&CK®
  - 4.4 Identifizierung neuer Arten von Angriffen
5. Regeln, Vorschriften und Strafverfolgung
  - 5.1 Cyber-Gesetze
  - 5.2 Compliance und Strafverfolgung
6. Risiko-Management
  - 6.1 Veränderte Herangehensweisen an das Risikomanagement
  - 6.2 Reaktion auf Zwischenfälle und Krisenmanagement
  - 6.3 Berücksichtigung der Black Swan Events
  - 6.4 Kontinuierliche Neubewertung
7. Threat Mitigation
  - 7.1 Defensive Taktiken und Technologien
  - 7.2 Strategien zur Risikominderung
  - 7.3 Validierung des Abwehrschutzes
  - 7.4 Sicherheit und Privacy by Design
  - 7.5 Implementierung von Mechanismen zur Verminderung der Bedrohungen in einer Organisation

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- CAPEC: Common Attack Pattern Enumeration and Classification. <https://capec.mitre.org/>
- Kim, P. (2014): The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC.
- Kim, P. (2015): The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC.
- Kim, P. (2018): The Hacker Playbook 3: Practical Guide to Penetration Testing. Secure Planet LLC.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- Pfleeger, C. P. / Pfleeger, S. L. / Margulies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input checked="" type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# Projekt: Threat Modeling

Kurscode: DLBCSEEF202\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01; DLBCSEEF201_D oder DLBCSEEF201_E

## Beschreibung des Kurses

Die Bedrohungen für moderne Computersysteme sind vielfältig und entwickeln sich ständig weiter. In diesem Projekt hat der Studierende die Gelegenheit, die Kunst und Wissenschaft der Bedrohungsmodellierung auf ein Szenario anzuwenden, das vom Dozenten zusammen mit dem Studierenden definiert wird. Die Grundlage bilden reale oder fiktive Fallstudien, zu denen der Studierende unter Verwendung einer geeigneten Methodik die Bedrohungen identifizieren und darüber berichten soll. Diese kann aus Methoden wie Attack Trees, STRIDE, DREAD oder einer gerechtfertigten Aufzählung von CAPEC oder Mitre ATT&CK® TTPs ausgewählt werden, je nachdem, was der Kursteilnehmer für am geeignetsten hält. Die Ergebnisse werden in Form eines Berichts präsentiert.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihr Wissen über die Modellierung von Bedrohungen auf Fälle und Szenarien anzuwenden.
- ihr daraus resultierendes Modell auf der Grundlage einer soliden Argumentation und in Bezug auf bekannte Techniken, Taktiken und Verfahren der Angreifer zu rechtfertigen.
- einen Bericht zu verfassen, der ihre Argumentation in systematischer und verständlicher Weise darlegt.

## Kursinhalt

- Für einen bestimmten Fall oder ein bestimmtes Szenario modellieren Studierende die Bedrohungen unter Verwendung einer etablierten Methodik und reicht dann den Bericht und, falls zutreffend, alle Codes und Daten ein. Spezifische Probleme und Kontexte werden vom Tutor vorgegeben, Vorschläge der Studierenden können jedoch berücksichtigt werden.

**Literatur**

**Pflichtliteratur**

**Weiterführende Literatur**

- Case Studies (Cyber): <https://www.securitymagazine.com/topics/2664-case-studies-cyber>
- Karger, P. A. / Scherr, R. R. (1974): MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS.
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 40 (3):769.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.
- Van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

DLBCSEEF02\_D



## Cloud Security

Module Code: DLBCSEECs\_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	<ul style="list-style-type: none"> <li>▪ DLBDSCC01 or DLBDSCC01_D</li> <li>▪ DLBDSCC01 or DLBDSCC01_D, DLBCSEECs01_E</li> </ul>	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

### Module Coordinator

Prof. Dr. Ahmed Taha (Security Controls in the Cloud) / N.N. (Project: Security by Design in the Cloud)

### Contributing Courses to Module

- Security Controls in the Cloud (DLBCSEECs01\_E)
- Project: Security by Design in the Cloud (DLBCSEECs02\_E)

### Module Exam Type

#### Module Exam

#### Split Exam

##### Security Controls in the Cloud

- Study Format "Distance Learning": Exam, 90 Minutes

##### Project: Security by Design in the Cloud

- Study Format "Distance Learning": Written Assessment: Project Report

### Weight of Module

see curriculum

**Module Contents****Security Controls in the Cloud**

- Cloud security
- Losing the intranet
- Security by design
- Secure cloud coding
- Confidentiality aspects
- Monitoring and Audit

**Project: Security by Design in the Cloud**

This module is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

**Learning Outcomes****Security Controls in the Cloud**

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

**Project: Security by Design in the Cloud**

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

**Links to other Modules within the Study Program**

This module is similar to other modules in the fields of Computer Science & Software Development

**Links to other Study Programs of the University**

All Bachelor Programs in the IT & Technology fields

## Security Controls in the Cloud

Course Code: DLBCSE ECS01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D

### Course Description

Maintaining a datacenter is expensive and inflexible, so it is expected that most corporations will be moving their server-based processes to a private, public or hybrid cloud in the next few years. Doing so will make operations more flexible and elastic but poses challenges to security architectures and operations. The paradigm of Infrastructure as Code (IaC) has been embraced by cloud providers and is a great opportunity to architect security into the design of a system (security by design) utilizing security best practices. However, too often, we see the on-premises mentality being applied to cloud deployments resulting in less secure systems instead of utilizing the security advantages a cloud provides. This course teaches the principles of Cloud Native security and how to avoid common pitfalls.

### Course Outcomes

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

### Contents

1. Cloud security is different
  - 1.1 Shared responsibility model
  - 1.2 Infrastructure as code
  - 1.3 The Private, Public and Hybrid Cloud
  - 1.4 Types of virtualization
  - 1.5 Cloud threat models: Mitre Cloud ATT&CK
2. Losing the intranet
  - 2.1 Identify and Access Management
  - 2.2 Principle of least privilege and fine-grained cloud access control
  - 2.3 Using Software Defined Networks, virtual private clouds and subnets
  - 2.4 Moving to a serverless architecture
  - 2.5 Defense in depth

3. Security by design
  - 3.1 Orchestration: Infrastructure as Code
  - 3.2 The Automate-Everything principle, Updating and Repeatability
  - 3.3 Reuse of good design patterns
  - 3.4 Container security
  - 3.5 Identification and Authentication
4. Secure cloud coding
  - 4.1 Software supply chain security
  - 4.2 Continuous Integration and Deployment
  - 4.3 Testing in code integration for security
  - 4.4 Canaries in code deployment
  - 4.5 Policy engines
5. Confidentiality aspects
  - 5.1 Secrets management
  - 5.2 Encryption of data at rest
  - 5.3 Encryption of data in transit
  - 5.4 Data leakage and exfiltration
6. Availability
  - 6.1 Storage tiers and locality
  - 6.2 Backup strategies
  - 6.3 Data and process redundancy
  - 6.4 Data lifecycle configuration
  - 6.5 DDoS mitigation
7. Locality
  - 7.1 Compliance requirements
  - 7.2 Geography of data/processes
  - 7.3 Redundancy of data centers
  - 7.4 Colocation for performance reasons
8. Monitoring and Audit
  - 8.1 Centralized logging
  - 8.2 Auditing orchestration scripts
  - 8.3 Detecting misconfigurations
  - 8.4 Cloud Forensics

9. Summary and Research topics
  - 9.1 Homomorphic encryption
  - 9.2 Attestation
  - 9.3 Proof-carrying data
  - 9.4 Side-channel attacks
  - 9.5 Conclusions

**Literature****Compulsory Reading****Further Reading**

- Mitre Cloud ATT&CK. <https://attack.mitre.org/matrices/enterprise/cloud/>

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides

## Project: Security by Design in the Cloud

Course Code: DLBCSE ECS02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSE ECS01_E

### Course Description

This course provides the opportunity to implement a cloud software system using best cloud security practices. A list of ideas is provided on the online learning platform. In addition, the students can contribute use case ideas of their own after consulting with the tutor. The core aim is to apply the theoretical knowledge of cloud security methods and best practices to implement an application that is deployed as an Infrastructure-as-code project, can be monitored and audited, as well as easily and preferably automatically updated without danger. This entails reasoning about possible design and architectural choices in a rational way, as well as implementing them on a cloud platform, such as CNCF, Amazon AWS, Microsoft Azure or Google GCP.

### Course Outcomes

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

### Contents

- This course is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

### Literature

#### Compulsory Reading

#### Further Reading

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Project
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Project Report

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides



# Pentesting

Module Code: DLBCSEPT\_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	<ul style="list-style-type: none"> <li>▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D</li> <li>▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEPT01_E</li> </ul>	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

## Module Coordinator

Enno Nagel (Principles of Ethical Hacking) / N.N. (Project: Pentesting)

## Contributing Courses to Module

- Principles of Ethical Hacking (DLBCSEPT01\_E)
- Project: Pentesting (DLBCSEPT02\_E)

## Module Exam Type

Module Exam	Split Exam
	<p><u>Principles of Ethical Hacking</u></p> <ul style="list-style-type: none"> <li>• Study Format "Distance Learning": Exam, 90 Minutes</li> </ul> <p><u>Project: Pentesting</u></p> <ul style="list-style-type: none"> <li>• Study Format "Distance Learning": Written Assessment: Project Report</li> </ul>

**Weight of Module**

see curriculum

**Module Contents****Principles of Ethical Hacking**

- Introduction to Ethical Hacking
- Reconnaissance
- Enumeration and Vulnerability Analysis
- Hacking Systems
- Malware

**Project: Pentesting**

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system.

**Learning Outcomes****Principles of Ethical Hacking**

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

**Project: Pentesting**

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

**Links to other Modules within the Study Program**

This module is similar to other modules in the fields of Computer Science & Software Development

**Links to other Study Programs of the University**

All Bachelor Programs in the IT & Technology fields

# Principles of Ethical Hacking

Course Code: DLBCSEPT01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D

## Course Description

Ethical hacking is an essential part in testing security implementations as well as discovering overlooked security issues. In this course, we will look at the principles and tools that hackers use and how ethical hacking is effectively utilized.

## Course Outcomes

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

## Contents

1. Introduction to Ethical Hacking
  - 1.1 Overview of Cyber Security
  - 1.2 Concepts of Cyber Kill Chain
  - 1.3 Hacking vs Ethical Hacking
  - 1.4 Laws and Standards
2. Reconnaissance
  - 2.1 Footprinting Techniques
  - 2.2 Network Scanning
  - 2.3 Host Discovery
  - 2.4 Service, Port and OS Discovery
  - 2.5 Scan beyond Security Measures

3. Enumeration and Vulnerability Analysis
  - 3.1 Enumeration Techniques
  - 3.2 Enumeration Countermeasures
  - 3.3 Vulnerability Assessment Techniques
  - 3.4 Vulnerability Classification and Assessment
4. Hacking Systems
  - 4.1 Gaining Access to Systems
  - 4.2 Privilege Escalation
  - 4.3 Persistent Access
  - 4.4 Covering Traces
5. Malware
  - 5.1 Types of Malware
  - 5.2 Concepts of Fileless Malware
  - 5.3 Countermeasures
6. Sniffing
  - 6.1 Concepts of Sniffing
  - 6.2 Sniffing Techniques
  - 6.3 Countermeasures
7. Denial of Service
  - 7.1 Concepts of DoS/DDoS
  - 7.2 Attack Techniques
  - 7.3 Botnets
  - 7.4 Countermeasures
8. Social Engineering
  - 8.1 Concepts of Social Engineering
  - 8.2 Social Engineering Techniques
  - 8.3 Identity Theft and Impersonation
  - 8.4 Countermeasures

**Literature****Compulsory Reading****Further Reading**

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: <https://www.acsac.org/2002/papers/classic-multics-orig.pdf> [last accessed: 25 August 2020]).
- Mitre PreATT&CK. <https://attack.mitre.org/matrices/pre/>
- Mitre Enterprise ATT&CK. <https://attack.mitre.org/matrices/enterprise/>
- Mitre Mobile ATT&CK. <https://attack.mitre.org/matrices/mobile/>
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. <https://github.com/blaCkHatHacEEkr/PENTESTING-BIBLE>

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides

## Project: Pentesting

Course Code: DLBCSEPT02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEPT01_E

### Course Description

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system. Students write a report outlining the vulnerabilities found, the methods used and proposals for fixing that class of vulnerability.

### Course Outcomes

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

### Contents

- The student will be provided with virtual environments emulating corporate systems and an attacker machine with the necessary tools.

### Literature

#### Compulsory Reading

#### Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: <https://www.acsac.org/2002/papers/classic-multics-orig.pdf> [last accessed: 25 August 2020]).
- Mitre PreATT&CK. <https://attack.mitre.org/matrices/pre/>
- Mitre Enterprise ATT&CK. <https://attack.mitre.org/matrices/enterprise/>
- Mitre Mobile ATT&CK. <https://attack.mitre.org/matrices/mobile/>
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. <https://github.com/blaCkHatHacEEkr/PENTESTING-BIBLE>

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Project
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Project Report

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides



# Industrielle Systemsicherheit

Modulcode: DLBCSEEIST\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ DLBINGEIT01 oder DLBINGEIT01_E</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	---	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Marian Benner-Wickner (Grundlagen der industriellen Softwaretechnik) / N.N. (Sicherheit im Internet of Things)

## Kurse im Modul

- Grundlagen der industriellen Softwaretechnik (IGIS01)
- Sicherheit im Internet of Things (DLBCSEEIST01\_D)

## Art der Prüfung(en)

<b>Modulprüfung</b>	<b>Teilmodulprüfung</b>
	<p><u>Grundlagen der industriellen Softwaretechnik</u></p> <ul style="list-style-type: none"> <li>• Studienformat "Kombistudium": <i>Prüfungsart</i></li> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> <li>• Studienformat "myStudium": <i>Prüfungsart</i></li> </ul> <p><u>Sicherheit im Internet of Things</u></p> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> </ul>

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****Grundlagen der industriellen Softwaretechnik**

- Aufbau und Organisation von Informationssystemen
- Risiken und Herausforderungen der industriellen Softwaretechnik
- Softwarelebenszyklus: Von Planung bis Ablösung
- Requirements Engineering und Spezifikation
- Architektur und Implementierung
- Qualitätssicherung, Betrieb und Weiterentwicklung
- Rollen im Software Engineering
- Organisation von Softwareprojekten
- Softwareprozessmodell-Rahmenwerke

**Sicherheit im Internet of Things**

- Grundlagen des Internet der Dinge (IoT)
- Angriffe auf das Internet der Dinge
- Sicherheit durch Design
- Sichern von Geräten für das Internet der Dinge
- Operative Sicherheit
- Cloud-Sicherheit
- Große Daten / Künstliche Intelligenz

**Qualifikationsziele des Moduls****Grundlagen der industriellen Softwaretechnik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einfache Berechnungen im Binärsystem (Boolsche Algebra) durchzuführen.
- den Aufbau von Rechnersystemen und Kommunikationsnetzen zu beschreiben.
- die Phasen eines SW-Lebenszyklus voneinander abzugrenzen.
- Rollen und Phasen im Software-Prozess voneinander abzugrenzen.
- verschiedene Vorgehensmodelle der SW-Entwicklung zu kennen.
- typische Herausforderungen und Risiken der industriellen SW-Entwicklung zu kennen.
- verschiedene Programmierparadigmen und deren Einsatz zu kennen.

**Sicherheit im Internet of Things**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte von IoT-Architekturen zu kennen und zu verstehen.
- die gängigsten Schwachstellen, Bedrohungen und Risiken für das Internet der Dinge zu kennen und zu verstehen.
- Gegenmaßnahmen für IoT-Schwachstellen zu verstehen und anzuwenden.
- ein IoT-Architekturmodell/eine IoT-Lösung zu analysieren.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Grundlagen der industriellen Softwaretechnik

Kurscode: IGIS01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen Einblick in die technischen und theoretischen Grundlagen des Software Engineering zu vermitteln. Neben dem generellen Aufbau von Rechnersystemen werden den Studierenden typische Herausforderungen bei der Entwicklung industrieller Informationssysteme vermittelt. Darüber hinaus wird dargestellt, mit welchen typischen Phasen und Aktivitäten im Software Engineering diese Risiken gezielt adressiert werden.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einfache Berechnungen im Binärsystem (Boolsche Algebra) durchzuführen.
- den Aufbau von Rechnersystemen und Kommunikationsnetzen zu beschreiben.
- die Phasen eines SW-Lebenszyklus voneinander abzugrenzen.
- Rollen und Phasen im Software-Prozess voneinander abzugrenzen.
- verschiedene Vorgehensmodelle der SW-Entwicklung zu kennen.
- typische Herausforderungen und Risiken der industriellen SW-Entwicklung zu kennen.
- verschiedene Programmierparadigmen und deren Einsatz zu kennen.

## Kursinhalt

1. Aufbau und Organisation von Informationssystemen
  - 1.1 0 und 1 als Grundlage aller IT-Systeme
  - 1.2 Von-Neumann-Architektur
  - 1.3 Verteilte Systeme und Kommunikationsnetze
  - 1.4 Betriebliche Informationssysteme
2. Risiken und Herausforderungen der industriellen Softwaretechnik
  - 2.1 Eigenschaften von industriellen Softwaresystemen
  - 2.2 Softwaretechnik
  - 2.3 Risiken und typische Probleme
  - 2.4 Ursachenforschung
  - 2.5 Herausforderungen im Software Engineering

3. Softwarelebenszyklus: Von Planung bis Ablösung
  - 3.1 Der Softwarelebenszyklus im Überblick
  - 3.2 Planung
  - 3.3 Entwicklung
  - 3.4 Betrieb
  - 3.5 Wartung
  - 3.6 Abschaltung
4. Requirements Engineering und Spezifikation
  - 4.1 Requirements Engineering
  - 4.2 Spezifikation
5. Architektur und Implementierung
  - 5.1 Architektur
  - 5.2 Implementierung
6. Qualitätssicherung, Betrieb und Weiterentwicklung
  - 6.1 Qualitätssicherung
  - 6.2 Betrieb
  - 6.3 Weiterentwicklung
7. Rollen im Software Engineering
  - 7.1 Idee der rollenbasierten Herangehensweise
  - 7.2 Typische Rollen
8. Organisation von Softwareprojekten
  - 8.1 Vom Prozessparadigma zum Softwareprozess
  - 8.2 Prozessparadigmen
9. Softwareprozessmodell-Rahmenwerke
  - 9.1 V-Modell XT
  - 9.2 Rational Unified Process (RUP)
  - 9.3 Scrum

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Gumm, H. P./Sommer, M. (2011): Einführung in die Informatik. 9. Auflage, Oldenbourg, München.
- Hansen, H. R./Neumann, G. (2009): Wirtschaftsinformatik 1. Grundlagen und Anwendungen. 10. Auflage, UTB, Stuttgart.
- Ludewig, J./Lichter, H. (2010): Software Engineering. Grundlagen, Menschen, Prozesse, Techniken. 2. Auflage, dpunkt.verlag, Heidelberg.
- Sommerville, I. (2007): Software Engineering. 8. Auflage, Addison-Wesley, Boston.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b>
------------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b>
---------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

# Sicherheit im Internet of Things

Kurscode: DLBCSEEIST01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBINGEIT01 oder DLBINGEIT01_E

## Beschreibung des Kurses

Das Internet der Dinge (IoT) ist ein Megatrend. Er umfasst sowohl Endverbrauchersysteme als auch industrielle Systeme und Technologien (Industrial IoT, oder IIoT). Es gibt eine zunehmende Anzahl miteinander verbundener Geräte, aus denen sich das Internet der Dinge zusammensetzt. Im Allgemeinen besteht die Architektur des Internet der Dinge aus Endgeräten, Cloud-Lösungen und Akteuren/Sensoren. Die Sicherheit des Internet der Dinge bringt verschiedene Themen zusammen, d.h. Netzwerkprotokolle, Software, Hardware, Kryptographie und Cloud Computing.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte von IoT-Architekturen zu kennen und zu verstehen.
- die gängigsten Schwachstellen, Bedrohungen und Risiken für das Internet der Dinge zu kennen und zu verstehen.
- Gegenmaßnahmen für IoT-Schwachstellen zu verstehen und anzuwenden.
- ein IoT-Architekturmodell/eine IoT-Lösung zu analysieren.

## Kursinhalt

1. Grundlagen des Internet der Dinge (IoT)
  - 1.1 Einführung
  - 1.2 Architektur
  - 1.3 Nicht-industrielles Internet der Dinge
  - 1.4 Industrie 4.0 (Industrielles IoT)
2. Angriffe auf das Internet der Dinge
  - 2.1 Verwundbarkeiten, Bedrohungen und Risiken
  - 2.2 Cyber-Angriffe und Gegenmaßnahmen
3. Sicherheit durch Design
  - 3.1 Projektmanagement / Sicherer Lebenszyklus der Entwicklung
  - 3.2 Statische Prüfung
  - 3.3 Dynamische Prüfung
  - 3.4 DevSecOps

4. Sichern von Geräten für das Internet der Dinge
  - 4.1 Sicherheitsrisiken
  - 4.2 Entwurfsziele
5. Operative Sicherheit
  - 5.1 Informations- und Cyber-Sicherheitsverwaltungssystem
  - 5.2 Netzwerk-Sicherheit
  - 5.3 Gerätekonfiguration
  - 5.4 Authentifizierung und Autorisierung
6. Cloud-Sicherheit
  - 6.1 Konzept des Nebels
  - 6.2 Bedrohungen für Cloud Internet of Things-Dienste
  - 6.3 Cloudbasierte Sicherheitsdienste
  - 6.4 Sichern der Cloud-Lösung
7. Big Data / Künstliche Intelligenz
  - 7.1 Beaufsichtigtes Lernen
  - 7.2 Unbeaufsichtigtes Lernen

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Butun, I. (2020): Industrial IoT. Challenges, Design Principles, Applications, and Security. 1st Edition, Springer International Publishing, Cham.
- Gupta B./Quamara, M. (2020): Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. 1st edition, CRC Press, Boca Raton, FL.
- Liyanage, M. et al. (2020): IoT Security. Advances in Authentication. 1st edition, John Wiley & Sons Ltd., Hoboken, NJ.
- Russell, B./Van Duren, D. (2018): Practical Internet of Things Security. Design a security framework for an Internet connected ecosystem. 2nd edition, Packt Publishing Ltd., Birmingham.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

## Cyber Threat Intelligence

Module Code: DLBCSEECTI\_E

<b>Module Type</b> see curriculum	<b>Admission Requirements</b> <ul style="list-style-type: none"> <li>▪ none</li> <li>▪ DLBCSEECTI01_E</li> </ul>	<b>Study Level</b> BA	<b>CP</b> 10	<b>Student Workload</b> 300 h
--------------------------------------	--	--------------------------	-----------------	----------------------------------

<b>Semester / Term</b> see curriculum	<b>Duration</b>	<b>Regularly offered in</b> WiSe/SoSe	<b>Language of Instruction and Examination</b> English
--	-----------------	--	---

### Module Coordinator

Dr. Christian Prause (Attack Models and Threat Feeds) / N.N. (Project: Defense against APTs)

### Contributing Courses to Module

- Attack Models and Threat Feeds (DLBCSEECTI01\_E)
- Project: Defense against APTs (DLBCSEECTI02\_E)

### Module Exam Type

#### Module Exam

#### Split Exam

Attack Models and Threat Feeds

- Study Format "Distance Learning": Exam, 90 Minutes

Project: Defense against APTs

- Study Format "Distance Learning": Written Assessment: Project Report

### Weight of Module

see curriculum

**Module Contents****Attack Models and Threat Feeds**

- Threat actors
- Modeling an Attack
- Attack Preparation TTPs
- Enterprise TTPs
- Industrial Control Systems TTPs
- Reporting

**Project: Defense against APTs**

Using well-known methods like the MITRE ATT&CK Techniques, Tactics and Procedures students will be able to produce a comprehensive threat model. Therefore, students will have to determine through simulation or a “table top exercise” which data is already available and which external threat feed data is required. After analyzing the “attack side” students will utilize threat intelligence systems for diagnostic to do a gap analysis – especially what defense technology is missing – and will be able to give sound advice to enhance resilience and to foster response capabilities. Emphasis will be drawn on the practical aspects of the defense against a given threat actor using techniques including beyond technical solutions and determine what cooperation with CERTs and ISPs is required to effectively defend against threats.

**Learning Outcomes****Attack Models and Threat Feeds**

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

**Project: Defense against APTs**

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT’s, ISP’s and IT-Security companies.

**Links to other Modules within the Study Program**

This module is similar to other modules in the fields of Computer Science & Software Development

**Links to other Study Programs of the University**

All Bachelor Programs in the IT & Technology fields

## Attack Models and Threat Feeds

Course Code: DLBCSEECTI01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

### Course Description

In this course, we look in depth at modeling threats and using data to diagnose, analyze and make recommendations. After a broad look at threat actors, we look at a variety of ways of modeling threats. This spans from Attack Trees to Kill Chains, but whichever method works the best, it all boils down to adversary Techniques, Tactics and Procedures. We look into the various taxonomies of these as defined by Mitre's ATT&CK and determine what can be observed in data. It is rare that internal data is enough for a complete analysis and in practice the threat analyst must use external data sources. These are available in a variety of formats, but the industry is converging on STIX and the use of software platforms like ACT to do the parsing and provide a good user experience. After looking at examples of threat actors and reports on them, we tackle the problem of making recommendations and writing reports. In some cases, engaging with law enforcement is required in which case some particularities need to be observed.

### Course Outcomes

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

### Contents

1. Threat Actors
  - 1.1 Script Kiddies
  - 1.2 eCrime Threat Actors
  - 1.3 Advanced Persistent Threat Actors (APT)
  - 1.4 Threat Researchers
2. Modeling an Attack
  - 2.1 Phases of an Attack
  - 2.2 Lockheed Martin Kill-Chain
  - 2.3 Attack Trees
  - 2.4 Models for Security Risks and Cyber Attacks



3. Attack preparation TTPs
  - 3.1 Observability of Attack Preparations
  - 3.2 Operational Security of an Organization
4. Enterprise TTPs
  - 4.1 Behaviors of the Attacker
  - 4.2 Observable Data in an Enterprise
5. Industrial Control Systems TTPs
  - 5.1 Critical Infrastructure
  - 5.2 Special Considerations with IoT/ICS Defense
6. Threat data exchange
  - 6.1 Indicators of Compromise vs. Indicators of Attack
  - 6.2 Threat Intelligence Reports
  - 6.3 Ad-hoc Data Formats
  - 6.4 STIX Format, TAXII Protocol
  - 6.5 Semantics of Threat Data using Mitre ATT&CK, CVEs, etc.
7. Examples of Threat Analysis Platforms
  - 7.1 ACT Platform
  - 7.2 MISP
  - 7.3 OpenCTI
8. Examples of Threat Actors and their Modus Operandi
  - 8.1 Threat Model
  - 8.2 Relevant Indicator Data
  - 8.3 Relevant CTI Data
  - 8.4 Diagnosing the Threat
  - 8.5 Data Coverage Gap Analysis
9. Reporting
  - 9.1 Mapping Raw Data to Mitre ATT&CK
  - 9.2 Making Defensive Recommendations
  - 9.3 Writing Reports for Technical Staff
  - 9.4 Writing Reports for Management
  - 9.5 Working with Law Enforcement

**Literature****Compulsory Reading****Further Reading**

- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: <https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LMWhite-Paper-Intel-Driven-Defense.pdf>)
- MISP Platform: <https://www.misp-project.org/>
- Mitre ATT&CK. <https://attack.mitre.org/>
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Review Book
<input checked="" type="checkbox"/> Course Book	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Guideline
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Exam Template	<input checked="" type="checkbox"/> Slides

## Project: Defense against APTs

Course Code: DLBCSEECTI02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEECTI01_E

### Course Description

This project course will give students hands-on experience in the challenging task to analyze threat vectors and real attacks of highly sophisticated, well planned, prepared and conducted attack campaigns named “Advanced Persistent Threats – APT’s” which derive from state, non-state or highly criminal attackers. Students will need to consider all practical aspects of different attack vectors using technical and non-technical (like social engineering) methods and procedures. To have the right understanding how to defend against these attacks they will use an attack simulator like Foreseeti SecureCAD or AttackIQ or conduct a “table top exercise” to figure out what data is required to analyze what security components and system configurations are needed to defend against a given, highly capable threat actor. Through this course, students will develop a complete overview what technical applications can be used to enhance resilience, foster response capabilities and recover from such attacks. Furthermore, students will have to take into account so called “soft measures” like organizational and procedural policies and regulations, bearing in mind the human factor in its social and psychological form. Through the cooperation with CERT’s, ISP’s and IT-Security Companies, academics and state agencies, students will cooperate on international level with IT-experts and experts from other disciplines to improve their expertise and to develop their personality.

### Course Outcomes

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT’s, ISP’s and IT-Security companies.

### Contents

- This project course focuses on practical aspects how to defend against APTs. Students will start with a given use case to analyze a real-world APT Attack against a defined IT-System / Network, identify the different attack vectors on multiple levels and make the necessary data regarding used malware and exploits, techniques and procedures available by using a simulator or conducting a “table top exercise”. With this, students will develop a

comprehensive picture of vulnerabilities and security shortfalls in the IT-system / network of their own enterprise. Students will then have to analyze and identify what technical or non-technical measures could have prevented this attack using an interdisciplinary approach taking all levels and involved actors into account. Cooperation with other national and international CERT's, ISP, IT-Security companies and state agencies will be the basis for a sound assessment how to improve the own resilience using best practices, state of the art technologies and considering new technologies.

- All relevant artifacts and considerations are documented by the students in a comprehensive project report.

## Literature

### Compulsory Reading

### Further Reading

- ACT Platform: <https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/>
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: <https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>)
- MISP Platform: <https://www.misp-project.org/>
- Mitre PreATT&CK. <https://attack.mitre.org/matrices/pre/>
- Mitre Enterprise ATT&CK. <https://attack.mitre.org/matrices/enterprise/>
- Mitre Mobile ATT&CK. <https://attack.mitre.org/matrices/mobile/>
- Mitre ICS ATT&CK: [https://collaborate.mitre.org/attackics/index.php/Main\\_Page](https://collaborate.mitre.org/attackics/index.php/Main_Page)
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: <https://github.com/OpenCTI-Platform/opencti>
- Semantics of threat data: <http://www.ti-semantic.com>
- STIX: <https://www.oasis-open.org/standards#stix2.1>
- TAXII: <https://www.oasis-open.org/standards#taxii2.1>
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. <https://zeltser.com/cyber-threat-intel-and-ir-report-template/>

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Project
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Project Report

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Review Book
<input type="checkbox"/> Course Book	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Guideline
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input checked="" type="checkbox"/> Slides
<input type="checkbox"/> Exam Template	

# Telekommunikationspezifische Bedrohungen

Modulcode: DLBCSEEMT\_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	<ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ DLBIBRVS01 oder DLBIBRVS01_E;</li> <li>▪ DLBCSEINF01_D oder DLBCSEINF01_E</li> </ul>	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

N.N. (Funk- und Telekommunikationssicherheit) / N.N. (Softwarearchitektur mobiler Geräte)

## Kurse im Modul

- Funk- und Telekommunikationssicherheit (DLBCSEEMT01\_D)
- Softwarearchitektur mobiler Geräte (DLBCSEEMT02\_D)

## Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	<p><u>Funk- und Telekommunikationssicherheit</u></p> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> </ul> <p><u>Softwarearchitektur mobiler Geräte</u></p> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> </ul>
<p><b>Anteil der Modulnote an der Gesamtnote</b></p> <p>s. Curriculum</p>	

**Lehrinhalt des Moduls****Funk- und Telekommunikationssicherheit**

- Überblick über drahtlose Protokolle
- Grundlagen von Drahtlosen Netzwerken
- Telekommunikationsprotokoll-Klassen
- Telekom-Architektur
- Sicherheit von Handapparaten und Geräten
- Bedrohungen
- Andere drahtlose Anwendungen
- Schutzmaßnahmen

**Softwarearchitektur mobiler Geräte**

- Mobil-Technologie-Stacks
- Hardware
- Android-Betriebssystem
- Apple iOS-Betriebssystem
- Mobile Geräte
- Software-Ökosysteme und Sicherheit
- Bedrohungen von Mobiltelefone
- Verwaltung mobiler Geräte

**Qualifikationsziele des Moduls****Funk- und Telekommunikationssicherheit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen der bei der Datenübertragung verwendeten drahtlosen Signale zu verstehen.
- verschiedene Arten der drahtlosen Vernetzung zu identifizieren und ihre Unterschiede zu verstehen.
- Telekommunikationsterminologie zu verstehen und diese der IT-Terminologie gegenüberzustellen.
- Architekturen der wichtigsten drahtlosen Telekommunikationssysteme zu verstehen.
- Angriffsvektoren gegen mobile Geräte sowie das Kernnetzwerk zu verstehen.
- andere Arten der Vernetzung, die möglicherweise genutzt werden, zu finden.

**Softwarearchitektur mobiler Geräte**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Hardware- und Software-Stacks gängiger Mobiltelefone zu verstehen.
- die Sicherheitskontrollen in diesen Stacks verstehen.
- zu erkennen, welche Schutzmaßnahmen und Risiken mit den Ökosystemen der Geräte verbunden sind.
- zu erkennen, welche Angriffe in der Vergangenheit erfolgreich waren.
- die Verwaltung mobiler Endgeräte zum Schutz eines Unternehmens zu nutzen.



**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor -Programme im Bereich IT & Technik

# Funk- und Telekommunikationssicherheit

Kurscode: DLBCSEEMT01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch	-1	5	DLBIBRVS01 oder DLBIBRVS01_E; DLBCSEINF01_D oder DLBCSEINF01_E

## Beschreibung des Kurses

Die Zahl der Geräte, die drahtlos mit Netzwerken verbunden werden können, hat bereits die Zahl der Desktop- und Laptop-Computer überholt, die über ein Kabel mit einem lokalen Netzwerk verbunden sind. Vor allem Telefone und Tablets dominieren den Markt, die sich mit den drahtlosen Telekommunikationsnetzen verbinden. Es gibt aber auch viele andere Formen der drahtlosen Kommunikation, die von Geräten genutzt werden. Die Eigenheiten dieser drahtlosen Systeme müssen verstanden werden, um sie in ein vollständiges Sicherheitskonzept zu integrieren. Drahtlose Protokolle zwingen den User oft dazu, einem System zu vertrauen, in das er keinen Einblick hat. In diesem Kurs widmen wir uns genau diesem Thema.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen der bei der Datenübertragung verwendeten drahtlosen Signale zu verstehen.
- verschiedene Arten der drahtlosen Vernetzung zu identifizieren und ihre Unterschiede zu verstehen.
- Telekommunikationsterminologie zu verstehen und diese der IT-Terminologie gegenüberzustellen.
- Architekturen der wichtigsten drahtlosen Telekommunikationssysteme zu verstehen.
- Angriffsvektoren gegen mobile Geräte sowie das Kernnetzwerk zu verstehen.
- andere Arten der Vernetzung, die möglicherweise genutzt werden, zu finden.

## Kursinhalt

1. Überblick über drahtlose Protokolle
  - 1.1 Netzwerkprotokolle für den persönlichen Bereich (Bluetooth, RFID, NFC und andere)
  - 1.2 Protokolle für drahtlose lokale Netzwerke (802.11a,b, g, ac , p und weitere)
  - 1.3 Wide Area Network-Protokolle (Telekommunikationsprotokolle, LoRa, Satellitenprotokolle und mehr)
  - 1.4 Schlüsselaustausch und Kryptographie in drahtlosen Netzwerken

2. Grundlagen von Drahtlosen Netzwerken
  - 2.1 Frequenzen
  - 2.2 Modulationen
  - 2.3 Daten-Kodierungen
  - 2.4 Zielkonflikte
3. Telekommunikationsprotokoll-Klassen
  - 3.1 Telekommunikation vs. IT-Terminologie und -Technologien
  - 3.2 Telekommunikationsnormen
  - 3.3 Veraltete digitale Protokolle
  - 3.4 LTE
  - 3.5 5G
4. Telekom-Architektur
  - 4.1 Gesamtarchitektur
  - 4.2 Kern-Architektur
  - 4.3 Software-definierte Vernetzung
  - 4.4 5G-Campus-Netzwerke
  - 4.5 Sicherheit der Anwendungsschicht
5. Sicherheit von Handapparaten und Geräten
  - 5.1 Anforderungen
  - 5.2 Typischer Hardware-Entwurf
  - 5.3 IoT-Geräte
6. Bedrohungen
  - 6.1 Allgemeine Angriffsvektoren gegen (mobile) Geräte
  - 6.2 Allgemeine Angriffsvektoren gegen das Kernnetzwerk
  - 6.3 Mögliche Angriffe auf 5G-Campus-Netzwerke
7. Andere drahtlose Anwendungen
  - 7.1 Drahtlose Protokolle für Luftfahrt und Nautik
  - 7.2 Proprietäre Geräteprotokolle
  - 7.3 Großflächige Sensornetze (LoRa, Sigfox, ...)
  - 7.4 Digitale Sprach-/Datentechnologien (DECT/GAP, TETRA, ...)
  - 7.5 Satellitenkommunikation

- 8. Schutzmaßnahmen
  - 8.1 Mobile Technologie sicher integrieren
  - 8.2 Überwachung mobiler Geräte

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Bartock, M. / Cichonski, J. / Souppaya, M. (2020): 5G CYBERSECURITY: Preparing a Secure Evolution to 5G.
- Cichonski, J. / Franklin, J. M. / Bartock, M. (2017): Guide to LTE Security. NIST Special Publication 800-187.
- Mobile Threat Catalog, <https://pages.nist.gov/mobile-threat-catalogue/>
- Pavur, J. et al. (2020): A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In 2020 IEEE Symposium on Security and Privacy (S&P). IEEE. May, 2020.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

## Softwarearchitektur mobiler Geräte

Kurscode: DLBCSEEMT02\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

### Beschreibung des Kurses

Mobile Geräte haben Desktops und Laptops als häufigste Endbenutzergeräte verdrängt. Das Smartphone ist zu einem zentralen Geschäftsinstrument geworden und User verwenden sie täglich für die unterschiedlichsten Anwendungen. Darüber hinaus nutzt auch das Internet der Dinge (IoT) diese mobilen Plattformen. Doch allzu oft sind die mit diesen mobilen Geräten verbundenen Risiken und Chancen insbesondere für die Sicherheitsadministratoren undurchsichtig, da diese Geräte oft außerhalb des traditionellen Intranets betrieben werden. In diesem Kurs untersuchen wir, wie die dominierenden Akteure, Android und Apple iOS, mit der Sicherheit in ihrem Softwarestack und ihrem Ökosystem umgehen. Wir betrachten auch das übersehene Problem der IoT-Sicherheit und schließen mit organisatorischen Lösungen ab.

### Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Hardware- und Software-Stacks gängiger Mobiltelefone zu verstehen.
- die Sicherheitskontrollen in diesen Stacks verstehen.
- zu erkennen, welche Schutzmaßnahmen und Risiken mit den Ökosystemen der Geräte verbunden sind.
- zu erkennen, welche Angriffe in der Vergangenheit erfolgreich waren.
- die Verwaltung mobiler Endgeräte zum Schutz eines Unternehmens zu nutzen.

### Kursinhalt

1. Mobil-Technologie-Stacks
  - 1.1 Hardware
  - 1.2 Firmware
  - 1.3 Betriebssystem
  - 1.4 Bewerbungen
  - 1.5 Ökosystem

2. Hardware
  - 2.1 RF-Module
  - 2.2 PDA-Modul
  - 2.3 Trusted Execution Environment
  - 2.4 Biometrische Geräte
  - 2.5 Standorttechnik
3. Android-Betriebssystem
  - 3.1 Hardware
  - 3.2 Bootloader
  - 3.3 Kernel- und Hardware-Abstraktionsschicht
  - 3.4 Sandboxing und Virtualisierung
  - 3.5 Code-Unterzeichnung
4. Apple iOS-Betriebssystem
  - 4.1 Hardware
  - 4.2 Bootloader
  - 4.3 Kernel und Frameworks
  - 4.4 Sandboxing und Virtualisierung
  - 4.5 Code-Unterzeichnung
5. Mobile Geräte
  - 5.1 Das Internet der Dinge
  - 5.2 Linux
  - 5.3 RTOS
  - 5.4 Android auf Geräten
  - 5.5 Andere gebräuchliche eingebettete Betriebssysteme
6. Software-Ökosysteme und Sicherheit
  - 6.1 Google Play
  - 6.2 Apple Store
  - 6.3 Sicherheitsanbieter
  - 6.4 Die Rolle der Cloud
7. Bedrohungen von Mobiltelefonen
  - 7.1 Historische Beispiele für Angriffe auf Mobiltelefone
  - 7.2 Taxonomie der Bedrohungen von Mobiltelefonen
  - 7.3 Jailbreaking

- 8. Verwaltung mobiler Geräte
  - 8.1 Die Bedrohungen der BYOD
  - 8.2 Einzigartige Bedrohungen für mobile Geräte
  - 8.3 Verwaltung von Patches und Richtlinien

#### Literatur

##### Pflichtliteratur

##### Weiterführende Literatur

- Gupta, A. (2014): Learning Pentesting for Android Devices
- Mobile Threat Catalog, <https://pages.nist.gov/mobile-threat-catalogue/>
- N.A. (2020): Android Enterprise Security White Paper.
- N.A. (2019): iOS Security iOS 12.3. [https://www.apple.com/lae/business/docs/site/iOS\\_Security\\_Guide.pdf](https://www.apple.com/lae/business/docs/site/iOS_Security_Guide.pdf)
- Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBCSEEMT02\_D

# Apple Mobile Solution Development

Modulcode: DLAMSD

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	Für die Teilnahme an diesem Kurs wird ein Mac-Computer (z.B. MacBook, iMac) mit einem aktuellen macOS-Betriebssystem benötigt. Zur App-Entwicklung wird die im Mac-App-Store zur Verfügung gestellte Entwicklungsumgebung Xcode eingesetzt.	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

Prof. Dr. Sandra Rebholz (Apple Mobile Solution Development I) / Prof. Dr. Sandra Rebholz (Apple Mobile Solution Development II)

## Kurse im Modul

- Apple Mobile Solution Development I (DLAMSD01)
- Apple Mobile Solution Development II (DLAMSD02)

## Art der Prüfung(en)

<b>Modulprüfung</b>	<b>Teilmodulprüfung</b> <u>Apple Mobile Solution Development I</u> <ul style="list-style-type: none"> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul> <u>Apple Mobile Solution Development II</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>
<b>Anteil der Modulnote an der Gesamtnote</b> s. Curriculum	

<p><b>Lehrinhalt des Moduls</b></p> <p><b>Apple Mobile Solution Development I</b></p> <p>In diesem Kurs erhalten die Studierenden eine fundierte Einführung in die mobile App-Entwicklung auf der iOS-Plattform von Apple. Im Rahmen des Kurses lernen die Studierenden sowohl die grundlegenden Konzepte der objektorientierten Programmierung mit Swift kennen, als auch geeignete Methoden und professionelle Werkzeuge zum App-Design und zur App-Entwicklung.</p> <p><b>Apple Mobile Solution Development II</b></p> <p>In diesem Kurs befassen sich die Studierenden mit fortgeschrittenen Konzepten der mobilen App-Entwicklung auf der iOS-Plattform von Apple. Die Studierenden durchlaufen dabei den gesamten App-Design- und Entwicklungsprozess und nutzen aktuelle Frameworks und Best-Practices zum Entwurf und zur Umsetzung eigener interaktiver iOS-Apps.</p>
--

**Qualifikationsziele des Moduls****Apple Mobile Solution Development I**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte und Sprachkonstrukte der Programmiersprache Swift im Kontext eines Programms zu erklären.
- für vorgegebene Aufgabenstellungen einen passenden Algorithmus zu entwickeln und diesen in Form eines Swift-Programmes umzusetzen.
- geeignete Methoden und Werkzeuge zur App-Entwicklung mit Swift einzusetzen.
- den grundlegenden Aufbau einer iOS-App und deren Komponenten zu erläutern.
- eine einfache interaktive iOS-App zu entwickeln.

**Apple Mobile Solution Development II**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- fortgeschrittene Programmier Techniken zur Lösung praxisrelevanter Probleme anzuwenden.
- professionelle Werkzeuge und Methoden zur Entwicklung interaktiver Nutzerschnittstellen zu nutzen.
- relevante Software-Entwurfsmuster beim Design eigener iOS-Apps anzuwenden.
- geeignete Dienste und Programmierschnittstellen zur Umsetzung vorgegebener Anforderungen an eine mobile App auszuwählen und einzusetzen.
- interaktive iOS-Apps im Rahmen eines nutzerzentrierten Designprozesses zu konzipieren und zu entwickeln.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Apple Mobile Solution Development I

Kurscode: DLAMSD01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	Für die Teilnahme an diesem Kurs wird ein Mac-Computer (z.B. MacBook, iMac) mit einem aktuellen macOS-Betriebssystem benötigt. Zur App-Entwicklung wird die im Mac-App-Store zur Verfügung gestellte Entwicklungsumgebung Xcode eingesetzt.

## Beschreibung des Kurses

In diesem Kurs erarbeiten sich die Studierenden die Grundlagen zur mobilen App-Entwicklung auf der iOS-Plattform von Apple. Wesentliche Bestandteile dieses Kurses sind das Erlernen und Anwenden von grundlegenden Konzepten der objektorientierten Programmierung mit Swift sowie der Umgang mit professionellen Werkzeugen zum App-Design und zur App-Entwicklung. Anhand von praxisnahen Anwendungsbeispielen gewinnen die Studierenden einen Einblick in die Programmierung und die Entwicklung eigener iOS-Apps.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte und Sprachkonstrukte der Programmiersprache Swift im Kontext eines Programms zu erklären.
- für vorgegebene Aufgabenstellungen einen passenden Algorithmus zu entwickeln und diesen in Form eines Swift-Programmes umzusetzen.
- geeignete Methoden und Werkzeuge zur App-Entwicklung mit Swift einzusetzen.
- den grundlegenden Aufbau einer iOS-App und deren Komponenten zu erläutern.
- eine einfache interaktive iOS-App zu entwickeln.

## Kursinhalt

- In diesem Kurs erarbeiten sich die Studierenden die grundlegenden Konzepte der objektorientierten Programmierung anhand der Programmiersprache Swift. Im Kontext von praktischen Anwendungsbeispielen wenden die Studierenden die erlernten Sprachkonstrukte und Programmiertechniken an und nutzen professionelle Softwareentwicklungswerkzeuge, um eigene Programme zu implementieren, zu debuggen und zu testen. Zudem gewinnen die Studierenden im Rahmen des Kurses einen Einblick in die Entwicklung von iOS-Apps und deren grundlegenden Aufbau. In selbst durchgeführten

Projekten durchlaufen die Studierenden alle Schritte der App-Entwicklung und lernen dadurch den gesamten Entwicklungsprozess von der Konzeption bis zur Veröffentlichung einer iOS-App kennen.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Apple Education (2021): Develop in Swift Explorations. Xcode 12. (URL: <https://books.apple.com/book/id1556366287> [letzter Zugriff: 08.05.2021]).
- Manning, J./Buttfield-Addison, P. (2021): Head First Swift. O'Reilly Media, Inc., Farnham, UK.
- Sillmann, T. (2019): Das Swift Handbuch. Apps programmieren für macOS, iOS, watchOS und tvOS. Hanser, München.
- Swift.org (2021): The Swift Programming Language. Swift 5.4. (URL: <https://docs.swift.org/swift-book/index.html> [letzter Zugriff: 08.05.2021]).

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Projekt
------------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

# Apple Mobile Solution Development II

Kurscode: DLAMSD02

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	Für die Teilnahme an diesem Kurs wird ein Mac-Computer (z.B. MacBook, iMac) mit einem aktuellen macOS-Betriebssystem benötigt. Zur App-Entwicklung wird die im Mac-App-Store zur Verfügung gestellte Entwicklungsumgebung Xcode eingesetzt.

## Beschreibung des Kurses

In diesem Kurs erarbeiten sich die Studierenden fortgeschrittene Prinzipien der mobilen App-Entwicklung auf der iOS-Plattform von Apple. Der Fokus dieses Kurses liegt auf der Entwicklung interaktiver Nutzerschnittstellen unter Verwendung der dafür zur Verfügung stehenden Frameworks und Komponenten. Im Rahmen von eigenen Anwendungsprojekten wenden die Studierenden fortgeschrittene Programmiertechniken an und binden aktuelle Dienste und Schnittstellen zur Umsetzung innovativer App-Funktionen ein. Unter Nutzung moderner Software-Entwicklungswerkzeuge durchlaufen die Studierenden den vollständigen Prozess des Designs, der Implementierung und des Testens von interaktiven iOS-Apps.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- fortgeschrittene Programmiertechniken zur Lösung praxisrelevanter Probleme anzuwenden.
- professionelle Werkzeuge und Methoden zur Entwicklung interaktiver Nutzerschnittstellen zu nutzen.
- relevante Software-Entwurfsmuster beim Design eigener iOS-Apps anzuwenden.
- geeignete Dienste und Programmierschnittstellen zur Umsetzung vorgegebener Anforderungen an eine mobile App auszuwählen und einzusetzen.
- interaktive iOS-Apps im Rahmen eines nutzerzentrierten Designprozesses zu konzipieren und zu entwickeln.

## Kursinhalt

- In dem Kurs erarbeiten sich die Studierenden fortgeschrittene Konzepte der Programmiersprache Swift. Unter Anwendung eines nutzerzentrierten Design- und Entwicklungsprozesses konzipieren und entwickeln die Studierenden interaktive iOS-Apps. Die Studierenden wenden dabei die grundlegenden Prinzipien des Designs interaktiver Nutzerschnittstellen an und nutzen moderne Frameworks und Werkzeuge, um diese umzusetzen. Im Rahmen des Kurses erhalten die Studierenden einen umfassenden Einblick

in die Architektur einer iOS-App. Relevant sind in diesem Zusammenhang auch die Anwendung von gängigen Entwurfsmustern sowie der Prinzipien der ereignisgesteuerten Programmierung. Im Kontext eigener Anwendungsprojekte machen sich die Studierenden mit dem Umgang und der Einbindung von externen Diensten und Programmierschnittstellen vertraut, die zur Umsetzung spezieller App-Funktionen bereitstehen.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Apple Education (2021): Develop in Swift Fundamentals. Xcode 12. (URL: <https://books.apple.com/book/id1556365994> [letzter Zugriff: 08.05.2021]).
- Apple Education (2021): Develop in Swift Data Collections. Xcode 12. (URL: <https://books.apple.com/book/id1556365920> [letzter Zugriff: 08.05.2021]).
- Sillmann, T. (2019): Das Swift Handbuch. Apps programmieren für macOS, iOS, watchOS und tvOS. Hanser, München.
- Swift.org (2021): The Swift Programming Language. Swift 5.4. (URL: <https://docs.swift.org/swift-book/index.html> [letzter Zugriff: 08.05.2021]).

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Projekt
------------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLAMSD02

# IT-Sicherheitsberatung

Modulcode: DLBCSEEISC\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ DLBCSEEISC01_D oder DLBCSEEISC01_E</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	---	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

N.N. (Technische und betriebliche IT-Sicherheitskonzeptionen) / N.N. (Projekt: Einsatz und Konfiguration von SIEM-Systemen)

## Kurse im Modul

- Technische und betriebliche IT-Sicherheitskonzeptionen (DLBCSEEISC01\_D)
- Projekt: Einsatz und Konfiguration von SIEM-Systemen (DLBCSEEISC02\_D)

## Art der Prüfung(en)

### Modulprüfung

### Teilmodulprüfung

Technische und betriebliche IT-Sicherheitskonzeptionen

- Studienformat "Fernstudium": Klausur, 90 Minuten

Projekt: Einsatz und Konfiguration von SIEM-Systemen

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

### **Lehrinhalt des Moduls**

#### **Technische und betriebliche IT-Sicherheitskonzeptionen**

- Netzwerkanalyse und -auswertung
- Schutz-Profile
- Systeme der Intrusion Detection
- Netzwerk-Überwachung
- Sicherheitsinformationen und Ereignismanagement (SIEM)
- IT-Sicherheitsevaluierung und -bewertung

#### **Projekt: Einsatz und Konfiguration von SIEM-Systemen**

Dieser Projektkurs vermittelt den Studierenden praktische Erfahrungen mit der anspruchsvollen Aufgabe der Implementierung eines SIEM-Tools (Security Incident Event Management) in eine Unternehmens-IT-Umgebung. Die Studierenden müssen praktische Aspekte wie verschiedene Datenquellen, Datenfusion und Analysemethoden und -verarbeitung von große Datenmengen sowie Einschränkungen durch die Datenverfügbarkeit und unterschiedlichste Datenformate berücksichtigen:



**Qualifikationsziele des Moduls****Technische und betriebliche IT-Sicherheitskonzeptionen**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-Systeme und -Netzwerke zu analysieren und zu bewerten und Vulnerabilitäten aufzudecken.
- unternehmensspezifische "Schutzprofile" zu entwickeln.
- Tools für sensorbasierte Netzwerküberwachung, Intrusion Detection und Reaktionen darauf zu entwerfen und zu implementieren.
- "Big Data"-Fusionsmechanismen zu verwenden, den Sicherheitsstatus des IT-Systems und den Netzwerksicherheitsstatus zu bewerten und zu beurteilen und Maßnahmen zur Reaktion auf Vorfälle einzuleiten.
- den Sicherheitsstatus von IT-Systemen und Netzwerken zu bewerten und Ratschläge für Verbesserungen zu geben.

**Projekt: Einsatz und Konfiguration von SIEM-Systemen**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Herausforderungen bei der Integration eines SIEM in eine bestehende Unternehmens-IT-Infrastruktur zu verstehen.
- die technischen Grenzen zu bewerten, die mit dem Projekt der Implementierung und dem Betrieb eines SIEM verbunden sind.
- die für eine zuverlässige Ausführung des SIEM-Tools erforderlichen Komponenten zur Intrusions-Erkennung und -überwachung zu identifizieren.
- die Anforderungen hinsichtlich Datenerfassung, Datenfusion, -analyse und -verarbeitung zu analysieren.
- die Abweichung vom Normverhalten in IT-Systemen / Netzwerken zu identifizieren.
- eine eingehende Untersuchung von Malware-Proben einzuleiten und relevante Reaktionsstrategien anzuwenden - einschließlich automatisierter Antworten.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Technische und betriebliche IT-Sicherheitskonzeptio- nen

Kurscode: DLBCSEEISC01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

IT-Systeme und Netzwerke, die hochsensible Informationen und Daten enthalten und verarbeiten, sowie IT-Infrastruktur zur Unterstützung geschäftskritischer Prozesse oder nationaler kritischer Infrastrukturen erfordern höhere Sicherheitsmechanismen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. Basierend auf spezifischen "Schutzprofilen" müssen hoch entwickelte Tools, Mechanismen und Verfahren entworfen, implementiert, konfiguriert und betrieben werden. Mit diesem Kurs werden Studierende in der Lage sein, die gegebene IT-Infrastruktur zu bewerten, das Sicherheitsdesign neuer IT-Systeme und Netzwerke durch die Entwicklung spezifischer Schutzprofile zu unterstützen, und zu bewerten, welche technischen und betrieblichen Sicherheitsmaßnahmen und Anwendungen erforderlich sind und wie diese im Unternehmen integriert, konfiguriert und betrieben werden.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-Systeme und -Netzwerke zu analysieren und zu bewerten und Vulnerabilitäten aufzudecken.
- unternehmensspezifische "Schutzprofile" zu entwickeln.
- Tools für sensorbasierte Netzwerküberwachung, Intrusion Detection und Reaktionen darauf zu entwerfen und zu implementieren.
- "Big Data"-Fusionsmechanismen zu verwenden, den Sicherheitsstatus des IT-Systems und den Netzwerksicherheitsstatus zu bewerten und zu beurteilen und Maßnahmen zur Reaktion auf Vorfälle einzuleiten.
- den Sicherheitsstatus von IT-Systemen und Netzwerken zu bewerten und Ratschläge für Verbesserungen zu geben.

## Kursinhalt

1. Netzwerkanalyse und -auswertung
  - 1.1 Schichtspezifische Bedrohungen und Schwachstellen
  - 1.2 Daten-Fluss, Interdependenzen und Interrelationen
  - 1.3 Überprüfung und Erkennen von Schwachstellen
  - 1.4 Unterstützende Tools und Techniken

2. Schutz-Profile
  - 2.1 Referenzarchitektur, Technologie und Netzwerkbetrieb
  - 2.2 Risikobewertung, Restrisiko und Risikomanagement
  - 2.3 Sicherheitsanforderungen und Schutzmaßnahmen
  - 2.4 Sicherheitsbewertung von IT-Sicherheitsprodukten
  - 2.5 Akkreditierung von IT-Systemen und Netzwerken
3. Systeme der Intrusion Detection
  - 3.1 Erkennungsstrategie,
  - 3.2 Datenquellen, Sensoren
  - 3.3 Analytik
  - 3.4 Indikatoren für Kompromittierungen
4. Netzwerk-Überwachung
  - 4.1 Systeme zum Schutz vor Bedrohungen
  - 4.2 Technologie drahtloser Sensornetzwerke
  - 4.3 Austausch von Bedrohungsinformationen
5. Sicherheitsinformationen und Ereignismanagement (SIEM)
  - 5.1 Technische und betriebliche Daten-Quellen
  - 5.2 DATA-Fusion
  - 5.3 Normverhalten von Netzwerken
  - 5.4 Analyse großer Datenmengen - Übertragung technischer Daten in operative Informationen
  - 5.5 IT- Sicherheitslage und Lagebewusstsein
  - 5.6 Strategien zur Reaktion auf Vorfälle und automatisierte Gegenmaßnahmen
6. IT-Sicherheitsevaluierung und -bewertung
  - 6.1 IT-Sicherheits-Metriken
  - 6.2 Bewertung der IT-Sicherheit

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Bundesamt Für Sicherheit in der Informationstechnik und ConSecur GmbH - Einführung von Intrusion-Detection-Systemen, 31. Oktober 2002 - [www.bsi.bund.de](http://www.bsi.bund.de)
- Wolfgang Röck, Netzwerksicherheit und Intrusion Detection: Implementierung und Evaluierung eines Intrusion Detection Systems auf Basis des Open Source Systems Snort (Deutsch) Taschenbuch – 30. Januar 2009
- IT-Grundschutz Profiles - Structural Description - COMMUNITY DRAFT - © Federal Office for Information Security (BSI) 2018
- Martin Kappes, Netzwerk- und Datensicherheit ISBN: 3658161264 mEAN: 9783658161262 Eine praktische Einführung. 3., akt. und erweiterte Aufl. 2019
- David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask, Security Information and Event Management (SIEM) Implementation ©2011 The MacGraw-Hill Companies ISBN:978-0-07-170108-2
- Lance Hayden, Publication: Cover Image. · Book, IT Security Metrics: A PracticalFramework for Measuring Security & Protecting Data. 1st McGraw-Hill Education Group ©2010
- Chris McNab, Network Security Assessment

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

## Projekt: Einsatz und Konfiguration von SIEM-Systemen

Kurscode: DLBCSEEISC02\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSEEISC01_D oder DLBCSEEISC01_E

### Beschreibung des Kurses

Dieser Projektkurs vermittelt den Studierenden praktische Erfahrungen mit der anspruchsvollen Aufgabe der Implementierung eines SIEM-Tools (Security Incident Event Management) in eine Unternehmens-IT-Umgebung. Die Studierenden müssen praktische Aspekte wie verschiedene Datenquellen, Datenfusion und Analysemethoden und -verarbeitung von große Datenmengen sowie Einschränkungen durch die Datenverfügbarkeit und unterschiedlichste Datenformate berücksichtigen. Darüber hinaus stehen die Studierenden vor der Herausforderung, technische Daten in betriebliche Informationen zu übertragen, um die entsprechenden Gegenmaßnahmen einzuleiten. Durch diesen Kurs erhalten die Studenten einen ganzheitlichen Überblick über die Integration eines SIEM in eine Unternehmens-IT-Infrastruktur, sowie deren Anwendungen und Dienste.

### Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Herausforderungen bei der Integration eines SIEM in eine bestehende Unternehmens-IT-Infrastruktur zu verstehen.
- die technischen Grenzen zu bewerten, die mit dem Projekt der Implementierung und dem Betrieb eines SIEM verbunden sind.
- die für eine zuverlässige Ausführung des SIEM-Tools erforderlichen Komponenten zur Intrusions-Erkennung und -überwachung zu identifizieren.
- die Anforderungen hinsichtlich Datenerfassung, Datenfusion, -analyse und -verarbeitung zu analysieren.
- die Abweichung vom Normverhalten in IT-Systemen / Netzwerken zu identifizieren.
- eine eingehende Untersuchung von Malware-Proben einzuleiten und relevante Reaktionsstrategien anzuwenden - einschließlich automatisierter Antworten.

### Kursinhalt

- Dieser Projektkurs konzentriert sich auf praktische Aspekte der Implementierung eines SIEM in einer Unternehmens-IT-Infrastrukturumgebung. Die Studierenden beginnen mit einem ausgewählten Anwendungsfall und SIEM-System und evaluieren dann die Anforderungen, die erfüllt werden müssen, damit das SIEM-Systems als Teil eines Unternehmens-IT-Systems / Netzwerkes eingesetzt werden kann. Die Studierenden müssen die Anforderungen in Bezug auf Sensoren, Netzwerküberwachung, Intrusion Detection, Datenfusion, Big Data Analytics und die Umsetzung technischer Daten in betriebliche Informationen evaluieren.

- Auf der Grundlage der verfügbaren Informationen werden geeignete Gegenmaßnahmen - einschließlich automatisierter Gegenmaßnahmen - identifiziert und verarbeitet.
- Alle relevanten Artefakte und Überlegungen werden von den Studierenden in einem Projektbericht dokumentiert.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask, Security Information and Event Management (SIEM) Implementation ©2011 The MacGraw-Hill Companies ISBN:978-0-07-170108-2
- Whitepaper: Die sieben Kernfunktionen analysegestützter SIEM-Lösungen - [www.splunk.com](http://www.splunk.com)
- H. B. Mitchell Multi-Sensor Data Fusion: An Introduction – Springer Verlag ISBN: 978-3642090677
- Al-Sakib Khan Pathan The State of the Art in Intrusion Prevention and Detection – CRC Press, Taylor&Francis Group

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input checked="" type="checkbox"/> Folien
<input type="checkbox"/> Musterklausur	



# Social Engineering

Modulcode: DLBCSEESE\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ DLBCSEESE01_D oder DLBCSEESE01_E</li> <li>▪ keine</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	---	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

N.N. (Social Engineering und Insider Threats) / N.N. (Projekt: Social Engineering)

## Kurse im Modul

- Social Engineering und Insider Threats (DLBCSEESE01\_D)
- Projekt: Social Engineering (DLBCSEESE02\_D)

## Art der Prüfung(en)

### Modulprüfung

### Teilmodulprüfung

Social Engineering und Insider Threats

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Fallstudie

Projekt: Social Engineering

- Studienformat "Fernstudium": Projektpräsentation

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

### **Lehrinhalt des Moduls**

#### **Social Engineering und Insider Threats**

- Methoden des Social Engineering
- Rechtliche Aspekte des Social Engineering
- Compliance, Verhaltenskodex
- Erkennung von Insider-Bedrohungen
- Sicherheitspolitik und -vorschriften
- Nationale und internationale Zusammenarbeit und Informationsaustausch

#### **Projekt: Social Engineering**

- Methoden des Social Engineering
- Rechtliche Aspekte des Social Engineering
- Compliance, Verhaltenskodex
- Erkennung von Insider-Threats
- Sicherheitspolitik und -vorschriften
- Nationale und internationale Zusammenarbeit und Informationsaustausch

**Qualifikationsziele des Moduls****Social Engineering und Insider Threats**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Social-Engineering-Methoden gegenüber IT-Systemen und Netzwerken und erkennen Schwachstellen im eigenen Unternehmen zu analysieren und zu bewerten.
- Unternehmensspezifische, technische und organisatorische Sicherheitsrichtlinien und -vorschriften zu bewerten.
- Tools für die Netzwerküberwachung zu entwerfen und zu implementieren, um die Anwendung von Sicherheitsrichtlinien und -vorschriften zu erkennen und zu protokollieren.
- "Big Data"-Fusions- und maschinelle Lernmechanismen zur Bewertung und Beurteilung des IT-Systemnetzwerks sowie des Sicherheitsstatus von Benutzern und Administratoren und zur Entscheidung und Einleitung von Reaktionsmaßnahmen einzusetzen, um sich von Social Engineering und durch Insider-Bedrohungen verursachten Vorfällen zu erholen.
- den Sicherheitsstatus und das Sicherheitsbewusstsein im Unternehmen auf allen Ebenen zu bewerten und Ratschläge für Verbesserungen zu geben.

**Projekt: Social Engineering**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Bedeutung des "menschlichen Faktors" im Hinblick auf die Sicherheit von IT-Systemen und Netzwerken in Unternehmen anzuerkennen und die rechtlichen Normen im Hinblick auf Social Engineering und die Erkennung von Insider-Bedrohungen zu berücksichtigen.
- den Sicherheitsrahmen zu analysieren und zu bewerten und Sicherheitslücken und -defizite zu ermitteln.
- organisatorische, technische und sicherheitstechnische Richtlinien und Vorschriften zu entwickeln und umzusetzen.
- Kampagnen zur Förderung des Sicherheitsbewusstseins zu entwickeln und durchzuführen, um die Widerstandsfähigkeit gegen die Anwendung von Methoden des Social Engineering zu erhöhen.
- mit verschiedenen Interessengruppen wie nationalen Sicherheitsbehörden, Sicherheitsunternehmen und Internetdiensteanbietern zusammenzuarbeiten.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

## Social Engineering und Insider Threats

Kurscode: DLBCSEESE01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

### Beschreibung des Kurses

IT-Systeme und Netzwerke, die hochsensible Informationen und Daten enthalten und verarbeiten, sowie IT-Infrastruktur zur Unterstützung geschäftskritischer Prozesse oder nationaler kritischer Infrastrukturen sind für Angreifer von großem Interesse, um Informationen zu erlangen (Cyber-Spionage), Informationen und Daten zu manipulieren oder zu zerstören sowie grundlegende Funktionen und Dienste zu unterbrechen, indem sie diese Systeme und Unternehmen kompromittieren. Ein Angriffsvektor richtet sich an die Benutzer und Betreiber, um diese Personen als Mithelfer zu missbrauchen, um Sicherheitsrichtlinien und Vorschriften zu brechen. Social Engineering oder soziale Manipulation wird von Gegnern häufig eingesetzt, um an die notwendigen Informationen zu gelangen, um IT-Infrastrukturen zu kompromittieren und ihre spezifischen Ziele zu erreichen. Der Einsatz von Methoden des Social Engineering kommt der sogenannten "Insider-Bedrohung" sehr nahe. Personen aus dem Inneren der Organisation handeln aus verschiedenen Gründen gegen die Sicherheitspolitik und -vorschriften ihres eigenen Unternehmens. Rache, Unzufriedenheit oder manchmal auch kriminelle Absichten sind Gründe für ein solches Verhalten. Eine Kombination aus Social Engineering und "feindlichen Insidern" ist ein Ass für alle Gegner. Daher müssen technische und organisatorische Maßnahmen entwickelt und umgesetzt werden, um solche Bedrohungen abzuwenden. Mit diesem Kurs sind die Studierenden in der Lage, Methoden des Social Engineering zu erkennen und Insider-Bedrohungen zu identifizieren. Sie sind in der Lage, präventive Sicherheitsrichtlinien und -vorschriften sowie reaktionsfähige Sicherheitsmaßnahmen zu entwickeln und umzusetzen, um diesen Bedrohungen zu begegnen.

**Kursziele**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Social-Engineering-Methoden gegenüber IT-Systemen und Netzwerken und erkennen Schwachstellen im eigenen Unternehmen zu analysieren und zu bewerten.
- Unternehmensspezifische, technische und organisatorische Sicherheitsrichtlinien und -vorschriften zu bewerten.
- Tools für die Netzwerküberwachung zu entwerfen und zu implementieren, um die Anwendung von Sicherheitsrichtlinien und -vorschriften zu erkennen und zu protokollieren.
- "Big Data"-Fusions- und maschinelle Lernmechanismen zur Bewertung und Beurteilung des IT-Systemnetzwerks sowie des Sicherheitsstatus von Benutzern und Administratoren und zur Entscheidung und Einleitung von Reaktionsmaßnahmen einzusetzen, um sich von Social Engineering und durch Insider-Bedrohungen verursachten Vorfällen zu erholen.
- den Sicherheitsstatus und das Sicherheitsbewusstsein im Unternehmen auf allen Ebenen zu bewerten und Ratschläge für Verbesserungen zu geben.

**Kursinhalt**

1. Methoden des Social Engineering
  - 1.1 Phishing, Spear Phishing und Dynamite Phishing
  - 1.2 Quid pro quo, Köder (Baiting), Medienköder (Media Dropping)
  - 1.3 Scareware, Betrugsmasche CEO-Fraud
  - 1.4 Pretexting, Tailgating
2. Rechtliche Aspekte des Social Engineering
  - 2.1 Compliance, Verhaltenskodex
  - 2.2 Identitätsdiebstahl
  - 2.3 Datenschutz
3. Detektion von Innentätern
  - 3.1 Techniken des Data Mining
  - 3.2 Methoden des Machine Learning
  - 3.3 Umfassendes Framework für die Detektion von und Reaktion bei Innentätern
  - 3.4 Tools für die Selbstbeurteilung
  - 3.5 Organisatorische Maßnahmen und Awareness
4. Sicherheitsrichtlinien und -vorschriften
  - 4.1 Organisatorisches Framework, Compliance, Verhaltenskodex
  - 4.2 Training und Awareness
  - 4.3 Schutz vertraulicher Informationen
  - 4.4 Sicherheitsüberwachung und Störfallreaktion

5. Nationale/r und internationale/r Zusammenarbeit und Informationsaustausch
  - 5.1 Zusammenarbeit mit Internet Service Providern (ISP) und Vertretern der IT-Sicherheit
  - 5.2 Austauschplattformen und Foren für Tactics, Techniques und Procedures (TTP) und Best Practices
  - 5.3 Zusammenarbeit mit nationalen Sicherheitsbehörden

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited, Brisbane.
- Company: TrustedSec. (Internet DEMO Version to subscribe)
- Hadnagy, C. (2012): Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe, MITP-Verlags GmbH & Co. KG, Frechen.
- Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, Oxford.
- Kennedy, D.: The Social-Engineer Toolkit (SET)
- Menger, A. (2016): IT-Sicherheit und Social Engineering. Grundlagen, Erscheinungsformen und Schutzmöglichkeiten. Hochschule Osnabrück.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Fallstudie

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

# Projekt: Social Engineering

Kurscode: DLBCSEESE02\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSEESE01_D oder DLBCSEESE01_E

## Beschreibung des Kurses

Dieser Projektkurs vermittelt den Studierenden praktische Erfahrungen mit der anspruchsvollen Aufgabe, Social Engineering-Angriffe zu verhindern und zu kontern und die Insider-Bedrohung für die IT-Systeme und -Netzwerke von Unternehmen zu beseitigen oder zumindest zu mindern. Die Studierenden müssen praktische Aspekte sozialer und psychologischer Herausforderungen - den so genannten "Human Factor" - sowie die Anwendung technischer Toolkits zur Erkennung von Angriffen berücksichtigen, die durch Social-Engineering-Methoden gesteuert oder von feindlichen Insidern verursacht werden. Im Rahmen dieses Kurses erhalten die Teilnehmer einen vollständigen Überblick über organisatorische, technische und verfahrenstechnische Maßnahmen, indem sie die Landschaft der Bedrohungsvektoren analysieren, Schwachstellen und Sicherheitslücken im Unternehmen identifizieren und praktische Sicherheitsrichtlinien und -vorschriften, einschließlich Kampagnen zur Förderung des Sicherheitsbewusstseins, entwickeln und umsetzen, um durch Social Engineering und Insider-Bedrohungen verursachte Vorfälle zu verhindern und sich von ihnen zu erholen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Bedeutung des "menschlichen Faktors" im Hinblick auf die Sicherheit von IT-Systemen und Netzwerken in Unternehmen anzuerkennen und die rechtlichen Normen im Hinblick auf Social Engineering und die Erkennung von Insider-Bedrohungen zu berücksichtigen.
- den Sicherheitsrahmen zu analysieren und zu bewerten und Sicherheitslücken und -defizite zu ermitteln.
- organisatorische, technische und sicherheitstechnische Richtlinien und Vorschriften zu entwickeln und umzusetzen.
- Kampagnen zur Förderung des Sicherheitsbewusstseins zu entwickeln und durchzuführen, um die Widerstandsfähigkeit gegen die Anwendung von Methoden des Social Engineering zu erhöhen.
- mit verschiedenen Interessengruppen wie nationalen Sicherheitsbehörden, Sicherheitsunternehmen und Internetdiensteanbietern zusammenzuarbeiten.

## Kursinhalt

- Dieser Projektkurs konzentriert sich auf praktische Aspekte zur Verhinderung, Aufdeckung und Abwehr von Angriffen, die durch Social Engineering ausgelöst werden, sowie auf die Bedrohung durch feindliche Insider. Die Studierenden beginnen mit einem ausgewählten



Anwendungsfall, um eine greifbare und erfolgreiche Social-Engineering-Kampagne zu analysieren, die Hauptangriffsvektoren zu identifizieren und zu lernen, wie verschiedene Aktivitäten auf mehreren Ebenen zusammenwirken, um das Ziel oder den Angreifer zu erreichen. Die Studierenden müssen den Sicherheitsrahmen des angegriffenen Unternehmens analysieren und die Schwachstellen und Defizite identifizieren, die den Social Engineering-Angriff erfolgreich ermöglichten.

- Unter Berücksichtigung des "menschlichen Faktors" sollen die Studierenden dann organisatorische und technische Sicherheitsrichtlinien entwickeln, um aufzuzeigen, wie ein bestimmter Angriff hätte verhindert und der Schaden vermieden oder gemildert werden können. Alle relevanten Artefakte und Überlegungen werden von den Studierenden in einem umfassenden Projektbericht dokumentiert.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Blokdyk, G. (2019). Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited.
- Company. TrustedSec. (Internet DEMO Version to subscribe)
- Gelles, M. G. (2016). Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann,.
- Hadnagy, C. (2012). Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe, MITP-Verlags GmbH & Co. KG.
- Menger, A. (2016): IT-Sicherheit und Social Engineering. Grundlagen, Erscheinungsformen und Schutzmöglichkeiten. Hochschule Osnabrück
- Michael Bartsch & Stefanie Frey (2018). Cybersecurity Best Practices : Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Fachmedien Wiesbaden.
- Thomas Liedtke (2022). Informationssicherheit: Möglichkeiten und Grenzen. Springer Berlin.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Projektpräsentation

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

## Host Forensics

Module Code: DLBCSEEHF\_E

<b>Module Type</b> see curriculum	<b>Admission Requirements</b> <ul style="list-style-type: none"> <li>▪ DLBCSEHSF01_E or DLBCSEHSF01_D</li> <li>▪ DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E</li> </ul>	<b>Study Level</b> BA	<b>CP</b> 10	<b>Student Workload</b> 300 h
--------------------------------------	---	--------------------------	-----------------	----------------------------------

<b>Semester / Term</b> see curriculum	<b>Duration</b> Minimum 1 semester	<b>Regularly offered in</b> WiSe/SoSe	<b>Language of Instruction and Examination</b> English
--	--	--	---

### Module Coordinator

N.N. (Static and Dynamic Malware Analysis) / N.N. (Seminar: Sandbox Interpretation)

### Contributing Courses to Module

- Static and Dynamic Malware Analysis (DLBCSEEHF01\_E)
- Seminar: Sandbox Interpretation (DLBCSEEHF02\_E)

### Module Exam Type

#### Module Exam

#### Split Exam

Static and Dynamic Malware Analysis

- Study Format "Distance Learning": Exam, 90 Minutes

Seminar: Sandbox Interpretation

- Study Format "Distance Learning": Written Assessment: Research Essay

### Weight of Module

see curriculum

**Module Contents****Static and Dynamic Malware Analysis**

- Objectives in Malware analysis
- Analysis Lab setup
- Tools of the trade
- Malware Classification
- Sandboxes
- Reversing
- Digging deeper

**Seminar: Sandbox Interpretation**

This course is about the practical application of Malware analysis techniques to real sandbox log files.

**Learning Outcomes****Static and Dynamic Malware Analysis**

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

**Seminar: Sandbox Interpretation**

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

**Links to other Modules within the Study Program**

This module is similar to other modules in the fields of Computer Science & Software Development

**Links to other Study Programs of the University**

All Bachelor Programs in the IT & Technology fields

# Static and Dynamic Malware Analysis

Course Code: DLBCSEEHF01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D

## Course Description

Malware is a top compromise vector in cyber attacks. Analyzing the attacking Malware gives the security analyst insights into the methodology and intension of the attacker. There are a number of ways that Malware can be analyzed and this course will introduce the most common ones.

## Course Outcomes

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

## Contents

1. Objectives in Malware analysis
  - 1.1 Forensics
  - 1.2 Root cause analysis
  - 1.3 Mitigation
2. Analysis Lab setup
  - 2.1 Stealth
  - 2.2 Isolation
  - 2.3 Honeypots
3. Tools of the trade
  - 3.1 Virtual machines
  - 3.2 Debugger
  - 3.3 Disassembler

4. Malware Classification
  - 4.1 Antivirus
  - 4.2 Virustotal
  - 4.3 Yara
  - 4.4 Clustering with PEID, TELFHASH, TLSH, SSDEEP, etc
5. Sandboxes
  - 5.1 Levels of interaction
  - 5.2 Instrumentation
  - 5.3 Online sandboxing services, Virustotal
  - 5.4 Scripting for sandboxes
  - 5.5 Corporate sandbox considerations
6. Reversing
  - 6.1 Unpacking, decrypting and de-obfuscation
  - 6.2 Debugging techniques
  - 6.3 Control flow analysis
  - 6.4 Library and system calls
7. Digging deeper
  - 7.1 Domain and IP information
  - 7.2 Analysis of Javascript code
  - 7.3 Memory forensics
  - 7.4 Kernel debugging rootkits
  - 7.5 Theoretical underpinnings of program analysis

**Literature****Compulsory Reading****Further Reading**

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing, Cham.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: <https://beginners.re/> (last accessed: 24 August 2020)

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Review Book
<input checked="" type="checkbox"/> Course Book	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Guideline
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Exam Template	<input checked="" type="checkbox"/> Slides

## Seminar: Sandbox Interpretation

Course Code: DLBCSEEHF02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E

### Course Description

In this course, we explore the most important tool in Malware analysis, the Sandbox and extract from the Sandbox logs the potential attacks exhibited by the Malware.

### Course Outcomes

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

### Contents

- This course is about the practical application of Malware analysis techniques to real sandbox log files and extract the indicators of compromise and Malware objectives into a report.

### Literature

#### Compulsory Reading

#### Further Reading

- Gregg, M. (2008): Build Your Own Security Lab: A Field Guide for Network Testing. Wiley, Hoboken, NJ.
- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.



**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Seminar
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Research Essay

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides

DLBCSEEHF02\_E

# DevSecOps

Modulcode: DLBCSEEDSO\_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	<ul style="list-style-type: none"> <li>IWNF01 oder IWNF01_E</li> <li>keine</li> </ul>	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

Prof. Dr. Markus Kleffmann (Techniken und Methoden der agilen Softwareentwicklung) /  
N.N. (Projekt: Agiles DevSecOps-Software-Engineering)

## Kurse im Modul

- Techniken und Methoden der agilen Softwareentwicklung (IWNF01)
- Projekt: Agiles DevSecOps-Software-Engineering (DLBCSEEDSO01\_D)

## Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	<p><u>Techniken und Methoden der agilen Softwareentwicklung</u></p> <ul style="list-style-type: none"> <li>Studienformat "myStudium": <i>Prüfungsart</i></li> <li>Studienformat "Fernstudium": Klausur, 90 Minuten</li> <li>Studienformat "Kombistudium": <i>Prüfungsart</i></li> </ul> <p><u>Projekt: Agiles DevSecOps-Software-Engineering</u></p> <ul style="list-style-type: none"> <li>Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****Techniken und Methoden der agilen Softwareentwicklung**

- Merkmale und Prinzipien von Agilität
- Agilität in kleinen Teams mit Scrum
- Agiles Portfolio- und Projektmanagement
- Agiles Anforderungs- und IT-Architekturmanagement
- Agiles Testen
- Agile Delivery and Deployment

**Projekt: Agiles DevSecOps-Software-Engineering**

Dieses Modul behandelt die grundlegenden Sicherheitsprinzipien für die Nutzung von DevOps in der Softwareentwicklung, auch bekannt als das DevSecOps-Paradigma. Anhand eines sicherheitsrelevanten Szenarios werden in diesem Modul gute DevSecOps-Praktiken wie die Definition von Sicherheitsgrundsätzen, Vorgehensweise zur Bedrohungsmodellierung und der Automatisierung von IT-Sicherheitsprozessen als Teil der Continuous Integration/Continuous Development (CI/CD)-Pipeline veranschaulicht.

**Qualifikationsziele des Moduls****Techniken und Methoden der agilen Softwareentwicklung**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Probleme und Risiken der industriellen SW-Entwicklung und ihre Konsequenzen für Entwicklungsprozesse zu analysieren und zu beurteilen.
- die Grundprinzipien des „No-Frills Software Engineering“ zu erläutern.
- Praxisszenarien zu analysieren und selbständig geeignete Methoden und Werkzeuge des „No-Frills Software Engineering“ anzuwenden.

**Projekt: Agiles DevSecOps-Software-Engineering**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Thread-Modellierung in DevOps-Szenarien anzuwenden.
- sich mit den relevanten Sicherheitsgrundsätzen von DevOps aus internationalen Standards und bewährten Praktiken der Industrie vertraut zu machen.
- die geeigneten Werkzeuge und Automatisierungsansätze für DevSecOps auszuwählen.
- die kontinuierliche Überwachung der Einhaltung in „Infrastructure-as-a-Code“ -Szenarien zu entwerfen.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Techniken und Methoden der agilen Softwareentwicklung

Kurscode: IWNF01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen vertiefenden Einblick in das Thema agile Softwareentwicklung zu vermitteln. Dazu werden zunächst die grundlegenden Merkmale und Prinzipien von Agilität vorgestellt und diskutiert. Danach wird dargestellt, wie kleine Projekt und Teams agiles Software-Engineering betreiben können und wie sich die agilen Prinzipien auf große Projekte übertragen und dort anwenden lassen. Anschließend werden agile Techniken für ausgewählte Kernaktivitäten im Software-Engineering vermittelt, wobei ein Schwerpunkt auf dem Gebiet Testen, Delivery und Deployment liegt.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Probleme und Risiken der industriellen SW-Entwicklung und ihre Konsequenzen für Entwicklungsprozesse zu analysieren und zu beurteilen.
- die Grundprinzipien des „No-Frills Software Engineering“ zu erläutern.
- Praxisszenarien zu analysieren und selbständig geeignete Methoden und Werkzeuge des „No-Frills Software Engineering“ anzuwenden.

## Kursinhalt

1. Merkmale und Prinzipien von Agilität
  - 1.1 Merkmale und Herausforderungen von Softwareprojekten
  - 1.2 Klassifikation von Unsicherheit
  - 1.3 Gegenüberstellung von agiler und klassischer Softwareentwicklung
  - 1.4 Prinzipien von Agilität
2. Agilität in kleinen Teams mit Scrum
  - 2.1 Grundlagen und allgemeiner Aufbau mit Scrum
  - 2.2 Zentrales Managementartefakt: Product Backlog
  - 2.3 Weitere Managementartefakte

3. Agiles Portfolio- und Projektmanagement
  - 3.1 Planungsebenen im agilen Projektmanagement
  - 3.2 Agiles Portfoliomanagement
  - 3.3 Organisation mehrerer Teams in einem Projekt
  - 3.4 Produkt- und Release-Planung
4. Agiles Anforderungs- und IT-Architekturmanagement
  - 4.1 Requirements Engineering in agilen Projekten
  - 4.2 Architekturmanagement in agilen Projekten
5. Agiles Testen
  - 5.1 Grundlagen und Anforderungen an die QS-Organisation
  - 5.2 Teststufen und Agilität
  - 5.3 Testautomatisierung
6. Agile Delivery and Deployment
  - 6.1 Grundlagen und Continuous Delivery Pipeline
  - 6.2 Continuous Build and Continuous Integration
  - 6.3 Akzeptanztests, Lasttests und Continuous Deployment

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Baumgartner, M. et al. (2013): Agile Testing. Der agile Weg zur Qualität. Hanser, München.
- Biffel, S. et al. (Hrsg.) (2005): Value-Based Software Engineering. Springer, Berlin/Heidelberg.
- Cockburn, A. (2007): Agile Software Development. The Cooperative Game. 2. Auflage, Addison-Wesley, Upper Saddle River (NJ).
- DeMarco, T. (2003): Bärenango. Mit Risikomanagement Projekte zum Erfolg führen. Hanser, München.
- Epping, T. (2011): Kanban für die Softwareentwicklung. Springer, Berlin/Heidelberg.
- Geirhos, M. (2011): IT-Projektmanagement. Was wirklich funktioniert – und was nicht. Galileo Computing, Bonn.
- Hummel, H. (2011): Aufwandsschätzungen in der Software- und Systementwicklung. Spektrum, Wiesbaden.
- Künneth, T. (2012): Android 4. Apps entwickeln mit dem Android SDK. Galileo Computing, Bonn.
- Link, J. (2005): Softwaretests mit JUnit. 2.Auflage, dpunkt.verlag, Heidelberg.
- Mangold, P. (2009): IT-Projektmanagement. 3. Auflage, Spektrum, Wiesbaden.
- Motzel, E./O. Pannenbäcker (1998): Projektmanagement-Kanon. Der deutsche Zugang zum Project Management Body of Knowledge. TÜV-Verlag, Köln.
- Pichler, R. (2007): Scrum. Agiles Projektmanagement erfolgreich einsetzen. dpunkt.verlag, Heidelberg. (2007)
- Röpstorff, S./Wiechmann, R. (2012): Scrum in der Praxis. Erfahrungen, Problemfelder und Erfolgsfaktoren. dpunkt.verlag, Heidelberg.
- Rubin, K. S. (2014): Essential Scrum. Umfassendes Scrum-Wissen aus der Praxis. mitp, Frechen.
- Tiemeyer, E. (2010): Handbuch IT-Projektmanagement, Vorgehensmodelle, Managementinstrumente, Good Practices. Hanser, München.
- Wirdemann, R. (2011): Scrum mit User Stories. 2. Auflage, Hanser, München.
- Wolff, E. (2014): Continuous Delivery. Der pragmatische Einstieg. dpunkt.verlag, Heidelberg.
- Wolf, H./Bleek/W.-G. (2010): Agile Softwareentwicklung. Werte, Konzepte und Methoden. 2. Auflage, dpunkt.verlag, Heidelberg.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b>
---------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b>
------------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

# Projekt: Agiles DevSecOps-Software-Engineering

Kurscode: DLBCSEEDSO01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IWNF01 oder IWNF01_E

## Beschreibung des Kurses

Trotz der breiten Akzeptanz von DevOps in der Industrie ist die Integration von Sicherheitsprinzipien in dieses Paradigma (d.h. DevSecOps) für e viele IT-Fachleute immer noch eine große Herausforderung. In diesem Kurs lernen die KursteilnehmerInnen grundlegende DevSecOps-Konzepte kennen, wie z.B. die Modellierung von Bedrohungen, die Definition von Sicherheitsgrundsätzen, die kontinuierliche Überwachung der Einhaltung und die Integration der Automatisierung von IT-Sicherheitsprozessen in DevOps.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Thread-Modellierung in DevOps-Szenarien anzuwenden.
- sich mit den relevanten Sicherheitsgrundsätzen von DevOps aus internationalen Standards und bewährten Praktiken der Industrie vertraut zu machen.
- die geeigneten Werkzeuge und Automatisierungsansätze für DevSecOps auszuwählen.
- die kontinuierliche Überwachung der Einhaltung in „Infrastructure-as-a-Code“ -Szenarien zu entwerfen.

## Kursinhalt

- Dieser Kurs behandelt die grundlegenden Sicherheitsprinzipien zur Nutzung des DevSecOps-Ansatzes in Softwaretechnologie Szenarien. Der Inhalt dieses Kurses veranschaulicht die Anwendung von DevSecOps, um die Sicherheit einer Organisation kontinuierlich und ganzheitlich zu verbessern, anstatt sich nur auf den Schutz der zugrundeliegenden Software-Infrastruktur zu konzentrieren (wie im Fall traditioneller, nicht-agiler Methoden). Durch die Präsentation von DevSecOps-Prinzipien wie Bedrohungsmodellierung, Definition von Sicherheitsgrundsätzen, Werkzeuge der Automatisierung von IT-Sicherheitsprozessen und kontinuierliche Überwachung der Einhaltung von Vorschriften wird dieser Kurs vermitteln, wie Sicherheit bei der Entwicklung eines Softwaretechnologie Produkts integriert werden kann.

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Johnson, E. (2020): Secure DevOps. A Practical Introduction. (URL: <https://www.sans.org/ondemand/course/secure-dev-ops-a-practical-introduction> [Retrieved: 15.08.2020]).
- Hsu, T. (2018): Hands-On Security in DevOps. Packt Publishing, UK.
- Microsoft. (2020): Secure DevOps. Making security principles and practices an integral part of DevOps while maintaining improved efficiency and productivity. (URL: <https://www.microsoft.com/en-us/securityengineering/devsecops> [Retrieved: 15.08.2020]).
- Schneider, C. (2015): Security DevOps. Staying secure in agile projects. (URL: <https://owaspappseceurope2015.sched.com/event/378l/security-devops-staying-secure-in-agile-projects> [Retrieved: 15.08.2020]).
- Yasar, H. (2016): An Introduction to Secure DevOps. Including Security in the Software Lifecycle. (URL: <https://insights.sei.cmu.edu/devops/2016/11/an-introduction-to-secure-devops-including-security-in-the-software-lifecycle.html> [Retrieved: 15.08.2020]).

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

DLBCSEEDS001\_D

## Sicherheit in komplexen Netzwerken

Modulcode: DLBCSEESCN\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ IAMG01 oder DLBCSEITPAM02</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	--	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Prof.Dr. Holger Klus (IT-Architekturmanagement) / N.N. (Projekt: IT-Sicherheitsarchitekturen)

### Kurse im Modul

- IT-Architekturmanagement (IAMG01)
- Projekt: IT-Sicherheitsarchitekturen (DLBCSEESCN01\_D)

### Art der Prüfung(en)

#### Modulprüfung

#### Teilmodulprüfung

##### IT-Architekturmanagement

- Studienformat "Fernstudium": Klausur, 90 Minuten
- Studienformat "Kombistudium": Klausur

##### Projekt: IT-Sicherheitsarchitekturen

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****IT-Architekturmanagement**

- Grundlagen und Begriffe zum Management von IT-Unternehmensarchitekturen
- IT-Anwendungsportfoliomanagement
- Architektur-Governance
- Modellierung von IT-Unternehmensarchitekturen
- Frameworks am Beispiel von TOGAF
- Referenzmodelle und Musterkataloge

**Projekt: IT-Sicherheitsarchitekturen**

Umsetzung und Dokumentation praktischer Fragen zur IT-Sicherheit im Rahmen des IT-Architekturmanagements.

**Qualifikationsziele des Moduls****IT-Architekturmanagement**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundprinzipien von IT-Strategie, IT-Governance und IT-Architekturmanagement zu kennen, diese zu erläutern und voneinander abzugrenzen.
- die typischen Aktivitäten des IT-Architekturmanagements, deren Zusammenhänge und deren Abhängigkeiten zu erläutern und voneinander abzugrenzen.
- geeignete Modelle des IT-Architekturmanagements zu erkennen, sie voneinander abzugrenzen und deren Verwendungszweck zu erläutern.
- die Elemente und Inhalte ausgewählter IT-Architekturframeworks sowie Referenzmodelle und Musterkataloge zu erkennen.

**Projekt: IT-Sicherheitsarchitekturen**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-Architektur-Management-Tools und -Techniken aus der Perspektive der IT-Sicherheit einzusetzen.
- eine IT-Architektur im Hinblick auf IT-Sicherheitslücken eigenständig zu analysieren.
- eine IT-Sicherheitsarchitektur zu entwerfen und sie in das gesamte IT-Architekturmanagement zu integrieren.
- Probleme im Spannungsfeld zwischen betrieblichen, finanziellen und Management-Bedürfnissen und IT-Sicherheitsanforderungen zu identifizieren und zu erklären.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik



# IT-Architekturmanagement

Kurscode: IAMG01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Neben konkreten IT-Projekten, z. B. die Neuentwicklung eines IT-Systems oder die Einführung einer Standardsoftware, muss für die organisationsweite IT-Infrastruktur – also die Menge aller eingesetzter IT-Hardware und -Softwaresysteme – ein strategisches Management eingesetzt werden. Diese Leitung obliegt dem IT-Unternehmensarchitekten, der das IT-Architekturmanagement betreibt. Seine Aufgabe ist die strategische Ausrichtung der IT-Infrastruktur an die Geschäfts- und IT-Strategie der Organisation. Dieser Kurs vermittelt typische Konzepte, Methoden, Vorgehensweisen und Modelle für die Aufgaben im Rahmen des IT-Architekturmanagements.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundprinzipien von IT-Strategie, IT-Governance und IT-Architekturmanagement zu kennen, diese zu erläutern und voneinander abzugrenzen.
- die typischen Aktivitäten des IT-Architekturmanagements, deren Zusammenhänge und deren Abhängigkeiten zu erläutern und voneinander abzugrenzen.
- geeignete Modelle des IT-Architekturmanagements zu erkennen, sie voneinander abzugrenzen und deren Verwendungszweck zu erläutern.
- die Elemente und Inhalte ausgewählter IT-Architekturframeworks sowie Referenzmodelle und Musterkataloge zu erkennen.

## Kursinhalt

1. Grundlagen und Begriffe zum Management von IT-Unternehmensarchitekturen
  - 1.1 IT-Unternehmensarchitektur
  - 1.2 Ziele von Enterprise Architecture Management
  - 1.3 Prozesse im Management von IT-Unternehmensarchitekturen
2. IT-Anwendungsportfoliomanagement
  - 2.1 Überblick über das IT-Anwendungsportfoliomanagement
  - 2.2 Anwendungshandbuch
  - 2.3 Portfolioanalyse
  - 2.4 Bebauungsplanung

3. Architektur-Governance
  - 3.1 Aufbauorganisation
  - 3.2 Entwicklung und Durchsetzung von Richtlinien
  - 3.3 Projektbegleitung
4. Modellierung von IT-Unternehmensarchitekturen
  - 4.1 Modelle im Kontext IT-Architekturmanagement
  - 4.2 Dokumentationsformen für Prozesse und Anwendungen
  - 4.3 Dokumentationsformen für Systeme und Technologien
5. Frameworks am Beispiel von TOGAF
  - 5.1 Grundlagen und Einsatz von IT-Architekturframeworks
  - 5.2 Überblick und Kategorien von EAM-Frameworks
  - 5.3 The Open Group Architecture Framework (TOGAF)
6. Referenzmodelle und Musterkataloge
  - 6.1 Referenzmodelle für Architekturen
  - 6.2 Musterkatalog für Gestaltung von EAM

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Hanschke, I. (2011): Enterprise Architecture Management. Einfach und effektiv. Hanser, München.
- Keller, W. (2012): IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung. 2. Auflage, dpunkt.verlag, Heidelberg.
- Keuntje, J. H./Barkow, R. (Hrsg.) (2010): Enterprise Architecture. Management in der Praxis. Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen.
- Ross, J. W./ Weill, P./Robertson, D. C. (2006): Enterprise Architecture as Strategy. Creating a Foundation for Business Execution. Harvard Business Review Press, Boston.
- Schwarzer, B. (2009): Einführung in das Enterprise Architecture Management. Verstehen – Planen – Umsetzen. Books on Demand, Norderstedt.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien

## Projekt: IT-Sicherheitsarchitekturen

Kurscode: DLBCSEESC01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IAMG01 oder DLBCSEITPAM02

### Beschreibung des Kurses

Unter Verwendung von Methoden und Techniken aus dem Bereich IT-Architekturmanagement bearbeiten die Studierenden in diesem Kurs selbständig eine praktische Fragestellung im Bereich der IT-Sicherheitsarchitektur. Am Ende des Kurses sind die Studierenden in der Lage, auf der Basis einer bestehenden IT-System- / Netzwerkarchitektur eine IT-Sicherheitsarchitektur selbstständig zu entwickeln.

### Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-Architektur-Management-Tools und -Techniken aus der Perspektive der IT-Sicherheit einzusetzen.
- eine IT-Architektur im Hinblick auf IT-Sicherheitslücken eigenständig zu analysieren.
- eine IT-Sicherheitsarchitektur zu entwerfen und sie in das gesamte IT-Architekturmanagement zu integrieren.
- Probleme im Spannungsfeld zwischen betrieblichen, finanziellen und Management-Bedürfnissen und IT-Sicherheitsanforderungen zu identifizieren und zu erklären.

### Kursinhalt

- Umsetzung und Dokumentation praktischer Fragen zur IT-Sicherheit im Rahmen des IT-Architekturmanagements. Typische Szenarien sind z.B. "Implementierung von IT-Sicherheitsgeräten in komplexen Netzwerken", "Gestaltung von Prozessen für Sicherheitsupdates und Patch-Management" und "Einsatz von Inhouse-Ressourcen oder Outsourcing von IT-Sicherheitsaufgaben".

**Literatur**

**Pflichtliteratur**

**Weiterführende Literatur**

- Bartsch, M. / Frey, S. (2014): Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Fachmedien, Wiesbaden.
- Müller, K.-R. (2014): IT-Sicherheit mit System. 5. Auflage, Springer Fachmedien, Wiesbaden.
- Pfister, M. (2019): Info Guard Swiss Cyber Security - In 3 einfachen (aber wichtigen) Schritten zur Enterprise IT-Sicherheitsarchitektur. (URL: [www.infoguard.ch](http://www.infoguard.ch) [zuletzt besucht am 22.08.2020]).

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input checked="" type="checkbox"/> Folien
<input type="checkbox"/> Musterklausur	

DLBCSEESCNO1\_D



## Network Forensics

Module Code: DLBCSEENF\_E

<b>Module Type</b> see curriculum	<b>Admission Requirements</b> <ul style="list-style-type: none"> <li>▪ DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E</li> <li>▪ DLBCSEINF01_E or DLBCSEINF01_D</li> </ul>	<b>Study Level</b> BA	<b>CP</b> 10	<b>Student Workload</b> 300 h
--------------------------------------	---	--------------------------	-----------------	----------------------------------

<b>Semester / Term</b> see curriculum	<b>Duration</b> Minimum 1 semester	<b>Regularly offered in</b> WiSe/SoSe	<b>Language of Instruction and Examination</b> English
--	--	--	---

### Module Coordinator

Dr. Rachel John Robinson (Protocols, Log- and Dataflow-Analysis in Depth) / N.N. (Seminar: Threat Hunting, Analysis and Incident Response)

### Contributing Courses to Module

- Protocols, Log- and Dataflow-Analysis in Depth (DLBCSEENF01\_E)
- Seminar: Threat Hunting, Analysis and Incident Response (DLBCSEENF02\_E)

### Module Exam Type

<b>Module Exam</b>	<b>Split Exam</b> <u>Protocols, Log- and Dataflow-Analysis in Depth</u> <ul style="list-style-type: none"> <li>• Study Format "Distance Learning": Exam, 90 Minutes</li> </ul> <u>Seminar: Threat Hunting, Analysis and Incident Response</u> <ul style="list-style-type: none"> <li>• Study Format "Distance Learning": Written Assessment: Research Essay</li> </ul>
--------------------	---

### Weight of Module

see curriculum

<p><b>Module Contents</b></p> <p><b>Protocols, Log- and Dataflow-Analysis in Depth</b></p> <ul style="list-style-type: none"> <li>▪ Network Basics</li> <li>▪ Operating System Logs</li> <li>▪ Packet Capturing and Analysis</li> <li>▪ Log Management</li> <li>▪ Preparation for Attacks</li> <li>▪ Intrusion Detection and Prevention System</li> </ul> <p><b>Seminar: Threat Hunting, Analysis and Incident Response</b></p> <ul style="list-style-type: none"> <li>▪ Mitre ATT&amp;CK TTPs</li> <li>▪ APT actors</li> <li>▪ Security coverage gap analysis</li> </ul>	
<p><b>Learning Outcomes</b></p> <p><b>Protocols, Log- and Dataflow-Analysis in Depth</b></p> <p>On successful completion, students will be able to</p> <ul style="list-style-type: none"> <li>▪ locate and evaluate security relevant log data.</li> <li>▪ operate a typical SIEM system.</li> <li>▪ create and understand SOC procedures.</li> <li>▪ report findings in written and machine readable forms.</li> </ul> <p><b>Seminar: Threat Hunting, Analysis and Incident Response</b></p> <p>On successful completion, students will be able to</p> <ul style="list-style-type: none"> <li>▪ understand Mitre ATT&amp;CK® Techniques, Tactics and Procedures.</li> <li>▪ understand how APT actors use combinations of these TTPs.</li> <li>▪ understand how Botnets and related Malware behave in networks.</li> <li>▪ examine where to find evidence of these TTPs.</li> <li>▪ explore datasets for threats not picked up by existing rules.</li> <li>▪ do a gap analysis on existing protections with respect to a given APT.</li> <li>▪ design mitigations to given TTPs.</li> </ul>	
<p><b>Links to other Modules within the Study Program</b></p> <p>This module is similar to other modules in the fields of Computer Science &amp; Software Development</p>	<p><b>Links to other Study Programs of the University</b></p> <p>All Bachelor Programs in the IT &amp; Technology fields</p>

## Protocols, Log- and Dataflow-Analysis in Depth

Course Code: DLBCSEENF01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D

### Course Description

Logging is done for a variety of diagnosis reasons, but these logs can be very useful in finding security incidents. In this course, we look at a variety of sources of log files. These range from operating system logs, to application logs and network traffic logs. Context and additional information also need to be collected. All this data is then consolidated in a Security Information and Event Management system where it can be analyzed and triaged for action. Finally, major incidents need to be documented and communicated to the relevant parties.

### Course Outcomes

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

### Contents

1. Introduction to Network Forensics
  - 1.1 Basics of Network Forensics
  - 1.2 Evidence Handling Standards
  - 1.3 Verification of Evidence
2. Network Basics
  - 2.1 Protocol Basics and Functionality
  - 2.2 Difference between the OSI Model and TCP/IP Architecture
  - 2.3 Basics of TCP and UDP including Ports and Protocols
  - 2.4 DNS, DHCP and ARP
3. Host-Side Artifacts
  - 3.1 Network-based Artifacts stored in the Operating Systems
  - 3.2 Services and Ports
  - 3.3 TCP Connection States
  - 3.4 Tools for extracting the Artifacts

4. Packet Capture and Analysis
  - 4.1 Capturing Packets
  - 4.2 Tools like TCPDump and Wireshark
  - 4.3 Analysis of captured Packets
5. Location Information
  - 5.1 Impact of Time Zones on Investigations
  - 5.2 Location Information from the Network
  - 5.3 Location-based Services with Web Applications
  - 5.4 Location Information from WiFi
6. Preparing for Attacks
  - 6.1 Manage Netflow Data
  - 6.2 Loggings
  - 6.3 Antivirus
  - 6.4 SIEM and Incident Response
7. Intrusion Detection and Prevention Systems
  - 7.1 Detection Styles
  - 7.2 Host-based versus Network-based
  - 7.3 Challenges with Intrusion Detection and Prevention Systems
  - 7.4 Firewall and Application Logs
8. Correlation of Data
  - 8.1 Synchronization of Time across Multiple Systems
  - 8.2 Log Aggregation and Management
  - 8.3 Importance of Timelines

#### Literature

#### Compulsory Reading

#### Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- NIST Special Publication 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides

## Seminar: Threat Hunting, Analysis and Incident Response

Course Code: DLBCSEENF02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E

### Course Description

Much of a security officer's work is with data where incidents need to be analyzed and countermeasures implemented. This course uses the Mitre ATT&CK® framework to reference TTPs (Techniques, Tactics and Procedures) that map to security events. Not all TTPs can be found in labeled security events, so Threat Hunting aims to go beyond ordinary incident response and find indicators of these TTPs also using other methods.

### Course Outcomes

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

### Contents

- In this seminar, we cover the subjects of incident response and threat hunting using the Mitre ATT&CK® framework and publicly available reports.

### Literature

#### Compulsory Reading

#### Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Seminar
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Research Essay

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides

DLBCSEENF02\_E



# Business Intelligence

Modulcode: IWBI

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	--	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

<b>Modulverantwortliche(r)</b> Dr. Peter Poensgen (Business Intelligence ) / Dr. Peter Poensgen (Projekt Business Intelligence)
--

<b>Kurse im Modul</b>
<ul style="list-style-type: none"> <li>▪ Business Intelligence (IWBI01)</li> <li>▪ Projekt Business Intelligence (IWBI02)</li> </ul>

<b>Art der Prüfung(en)</b>	
<b>Modulprüfung</b>	<b>Teilmodulprüfung</b>
	<p><u>Business Intelligence</u></p> <ul style="list-style-type: none"> <li>• Studienformat "myStudium": Klausur, 90 Minuten</li> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> <li>• Studienformat "Kombistudium": Klausur, 90 Minuten</li> </ul> <p><u>Projekt Business Intelligence</u></p> <ul style="list-style-type: none"> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>

**Anteil der Modulnote an der Gesamtnote**

s. Curriculum

**Lehrinhalt des Moduls****Business Intelligence**

- Motivation und Begriffsbildung
- Datenbereitstellung
- Data Warehouse
- Modellierung multidimensionaler Datenräume
- Analysesysteme
- Distribution und Zugriff

**Projekt Business Intelligence**

Mögliche Themengebiete für das BI-Projekt sind u.a. „Management von BI-Projekten, „Konzeption von multidimensionalen Datenmodellen“ sowie „Prototypische Umsetzung von kleinen BI-Anwendungen“.

**Qualifikationsziele des Moduls****Business Intelligence**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivation, Anwendungsfälle und Grundlagen für Business Intelligence zu erklären.
- Techniken und Methoden zur Bereitstellung und Modellierung von Daten sowie für BI relevante Arten von Daten zu benennen und zu erläutern sowie voneinander abzugrenzen.
- Techniken und Methoden zur Informationsgenerierung und -speicherung zu erläutern und auf Basis konkreter Anforderungen selbstständig geeignete Methoden auszuwählen.

**Projekt Business Intelligence**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine Lösung zu einer praktischen Fragestellung im Thema Business Intelligence zu konzipieren, prototypisch umzusetzen und die dabei erzielten Ergebnisse zu dokumentieren.
- typische Probleme und Herausforderungen in der Konzeption und praktischen Umsetzung kleiner BI-Lösungen zu benennen und zu erläutern.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Business Intelligence

Kurscode: IWBI01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Business Intelligence (BI) dient der Gewinnung von Informationen aus Unternehmensdaten, die sowohl für eine gezielte Unternehmenssteuerung als auch für die Optimierung von Geschäftsaktivitäten relevant sind. Im Rahmen dieses Kurses werden Techniken, Vorgehensweisen und Modelle zur Datenbereitstellung, Informationsgenerierung und -analyse sowie der Verteilung der gewonnenen Informationen vorgestellt und diskutiert. Sie werden danach in der Lage sein, die verschiedenen Themengebiete des Data Warehousing zu erläutern und Methoden bzw. Techniken für konkrete Anforderungen selbstständig auszuwählen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivation, Anwendungsfälle und Grundlagen für Business Intelligence zu erklären.
- Techniken und Methoden zur Bereitstellung und Modellierung von Daten sowie für BI relevante Arten von Daten zu benennen und zu erläutern sowie voneinander abzugrenzen.
- Techniken und Methoden zur Informationsgenerierung und -speicherung zu erläutern und auf Basis konkreter Anforderungen selbstständig geeignete Methoden auszuwählen.

## Kursinhalt

1. Motivation und Begriffsbildung
  - 1.1 Motivation und historische Entwicklung
  - 1.2 BI als Rahmenwerk
2. Datenbereitstellung
  - 2.1 Operative und dispositive Systeme
  - 2.2 Das Data-Warehouse-Konzept
  - 2.3 Architekturvarianten
3. Data Warehouse
  - 3.1 ETL-Prozess
  - 3.2 DWH und Data Mart
  - 3.3 ODS und Metadaten

4. Modellierung multidimensionaler Datenräume
  - 4.1 Datenmodellierung
  - 4.2 OLAP-Würfel
  - 4.3 Physische Speicherung
  - 4.4 Star- und Snowflake-Schema
  - 4.5 Historisierung
  
5. Analysensysteme
  - 5.1 Freie Datenrecherche und OLAP
  - 5.2 Berichtssysteme
  - 5.3 Modellgestützte Analysensysteme
  - 5.4 Konzeptorientierte Systeme
  
6. Distribution und Zugriff
  - 6.1 Informationsdistribution
  - 6.2 Informationszugriff

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Bachmann, R./Kemper, G. (2011): Raus aus der BI-Falle. Wie Business Intelligence zum Erfolg wird. 2. Auflage, mitp, Heidelberg.
- Bauer, A./Günzel, H. (2008): Data Warehouse Systeme. Architektur, Entwicklung, Anwendung. 3. Auflage, dpunkt.verlag, Heidelberg.
- Betz, R. (2015): Werde Jäger des verlorenen Schatzes. In: Immobilienwirtschaft, Heft 5, S. 1614–1164. (URL <https://www.haufe.de/download/immobilienwirtschaft-ausgabe-052015-immobilienwirtschaft-fachmagazin-fuer-management-recht-praxis-303530.pdf> [letzter Zugriff: 27.02.2017]).
- Bodendorf, F. (2006): Daten- und Wissensmanagement. 2. Auflage, Springer, Berlin.
- Chamoni, P./Gluchowski, P. (Hrsg.) (2006): Analytische Informationssysteme Business Intelligence-Technologien und -Anwendungen. Springer, Berlin.
- Engels, C. (2008): Basiswissen Business Intelligence. W3L, Herdecke/Witten.
- Gansor, T./Totok, A./Stock, S. (2010): Von der Strategie zum Business Intelligence Competency Center (BICC). Konzeption – Betrieb – Praxis. Hanser, München.
- Gluchowski, P./Gabriel, R./Dittmar, C. (2008): Management Support Systeme und Business Intelligence. Computergestützte Informationssysteme für Fach- und Führungskräfte. 2. Auflage, Springer, Berlin/Heidelberg.
- Grothe, M. (2000): Business Intelligence. Aus Informationen Wettbewerbsvorteile gewinnen. Addison-Wesley, München.
- Gutenberg, E. (1983): Grundlagen der Betriebswirtschaft, Band 1. Die Produktion. 18. Auflage, Springer, Berlin/Heidelberg/New York.
- Hannig, U. (Hrsg.) (2002): Knowledge Management und Business Intelligence. Springer, Berlin.
- Hansen, H.-R./Neumann, G. (2001): Wirtschaftsinformatik I. Grundlagen betrieblicher Informationsverarbeitung. 8. Auflage, Lucius & Lucius UTB, Stuttgart.
- Humm, B./Wietek, F. (2005): Architektur von Data Warehouses und Business Intelligence Systemen. In: Informatik Spektrum, S. 3–14. (URL: [https://www.fbi.h-da.de/fileadmin/personal/b.humm/Publikationen/Humm\\_\\_Wietek\\_-\\_Architektur\\_DW\\_\\_Informatik-Spektrum\\_2005-01\\_.pdf](https://www.fbi.h-da.de/fileadmin/personal/b.humm/Publikationen/Humm__Wietek_-_Architektur_DW__Informatik-Spektrum_2005-01_.pdf) [letzter Zugriff: 27.02.2017]).
- Kemper, H.-G./Baars, H./Mehanna, W. (2010): Business Intelligence – Grundlagen und praktische Anwendungen. Eine Einführung in die IT-basierte Managementunterstützung. 3. Auflage, Vieweg+Teubner, Stuttgart.
- Turban, E. et al. (2010): Business Intelligence. A Managerial Approach. 2. Auflage, Prentice Hall, Upper Saddle River (NJ).

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



# Projekt Business Intelligence

Kurscode: IWBI02

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Unter Anwendung bekannter Methoden und Techniken aus dem Themengebiet Business Intelligence bearbeiten die Studierenden in diesem Kurs selbstständig eine praktische Fragestellung. Zum Abschluss des Kurses können Sie selbstständig auf der Grundlage konkreter Anforderungen Business Intelligence-Anwendungen konzipieren und prototypisch umsetzen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine Lösung zu einer praktischen Fragestellung im Thema Business Intelligence zu konzipieren, prototypisch umzusetzen und die dabei erzielten Ergebnisse zu dokumentieren.
- typische Probleme und Herausforderungen in der Konzeption und praktischen Umsetzung kleiner BI-Lösungen zu benennen und zu erläutern.

## Kursinhalt

- Umsetzung und Dokumentation von praktischen Fragestellungen zum Einsatz von Business Intelligence-Anwendungen. Typische Szenarien sind beispielsweise „Management von BI-Projekten“, „Konzeption von multidimensionalen Datenmodellen“ und „Prototypische Umsetzung von kleinen BI-Anwendungen“.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Brenner, W./Uebernicketel, F. (2015): Design Thinking. Das Handbuch. Frankfurter Allgemeine Buch, Frankfurt a. M.
- Brown, T. (2008): Design Thinking. In: Harvard Business Review, Heft Juni, S. 84–95.
- Meinel, C./Weinberg, U./Krohn, T. (Hrsg.) (2015): Design Thinking Live. Wie man Ideen entwickelt und Probleme löst. Murmann, Hamburg.
- Uebernicketel, F./Brenner, W. (2016): Design Thinking. In: Hoffmann, C. P. et al. (Hrsg.): Business Innovation: Das St. Galler Modell. Springer, Wiesbaden, S. 243–265.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Projekt
------------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Projekt
---------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

## Future Threats

Modulcode: DLBCSEEF\_T\_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	<ul style="list-style-type: none"> <li>▪ IREN01 oder DLBCSRE01; DLBCSEEF_T01_D oder DLBCSEEF_T01_E</li> <li>▪ IREN01 oder DLBCSRE01</li> </ul>	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

### Modulverantwortliche(r)

N.N. (Threat Modeling) / N.N. (Projekt: Threat Modeling)

### Kurse im Modul

- Threat Modeling (DLBCSEEF\_T01\_D)
- Projekt: Threat Modeling (DLBCSEEF\_T02\_D)

### Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	<u>Threat Modeling</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> </ul> <u>Projekt: Threat Modeling</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>
<b>Anteil der Modulnote an der Gesamtnote</b> s. Curriculum	

**Lehrinhalt des Moduls****Threat Modeling**

- C.I.A. Denken und mehr
- Messung der Cyber-Bedrohung
- Modellierung von Bedrohungen
- Bibliotheken angreifen
- Regeln, Vorschriften und Strafverfolgung
- Risiko-Management
- Threat Mitigation

**Projekt: Threat Modeling**

Dieser Kurs behandelt die Theorie und Praxis des Auffindens und der Modellierung von Bedrohungen in einem bestimmten System, einer bestimmten Architektur oder einem bestimmten Szenario. Er behandelt Methoden und Quellen für übliche Bedrohungsmuster. In einem Projekt wird die Theorie in die Praxis umgesetzt, indem eine gegebene Situation auf Bedrohungen analysiert wird.

**Qualifikationsziele des Moduls****Threat Modeling**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- souverän mögliche Bedrohungsarten zu durchdenken.
- diese Bedrohungen mit Hilfe einer gebräuchlichen Modellierungsmethode zu modellieren.
- relevante Techniken, Taktiken und Verfahren in Bezug auf ein bestimmtes Szenario zu finden.
- das aus dem Bedrohungsmodell hervorgehende Risiko zu ermitteln.
- das Risiko durch die Implementierung von Änderungen des Designs zu mindern.

**Projekt: Threat Modeling**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihr Wissen über die Modellierung von Bedrohungen auf Fälle und Szenarien anzuwenden.
- ihr daraus resultierendes Modell auf der Grundlage einer soliden Argumentation und in Bezug auf bekannte Techniken, Taktiken und Verfahren der Angreifer zu rechtfertigen.
- einen Bericht zu verfassen, der ihre Argumentation in systematischer und verständlicher Weise darlegt.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Threat Modeling

Kurscode: DLBCSEEF01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01

## Beschreibung des Kurses

Wenn ein System oder eine Architektur geschaffen wird, ist es wichtig, dass mögliche Bedrohungen gleichzeitig bewertet werden. Durch die Verwendung sowohl von Modellierungsmethoden als auch von in der Vergangenheit beobachteten Angriffsmustern ist es möglich, ein neues oder bestehendes System auf Bedrohungen hin zu untersuchen. Aus dieser Analyse lassen sich Risiken und Maßnahmen zu deren Verminderung ableiten. Während die gebräuchlichsten Methoden auf den Angriffsbäumen und dem STRIDE-Modell basieren, werden bei der Angriffsmodellierung in letzter Zeit auch Repositorien von Angreifer-Techniken, -Taktiken und -Verfahren (TTP's) zur Inspiration herangezogen.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- souverän mögliche Bedrohungsarten zu durchdenken.
- diese Bedrohungen mit Hilfe einer gebräuchlichen Modellierungsmethode zu modellieren.
- relevante Techniken, Taktiken und Verfahren in Bezug auf ein bestimmtes Szenario zu finden.
- das aus dem Bedrohungsmodell hervorgehende Risiko zu ermitteln.
- das Risiko durch die Implementierung von Änderungen des Designs zu mindern.

## Kursinhalt

1. C.I.A. Denken und mehr
  - 1.1 Vertraulichkeit (Confidentiality)
  - 1.2 Integrität (Integrity)
  - 1.3 Verfügbarkeit (Availability)
  - 1.4 Sicherheit und andere Belange
2. Messung der Cyber-Bedrohung
  - 2.1 Messung und Verwaltung
  - 2.2 Metriken zur Cyber-Bedrohung
  - 2.3 Messung der Bedrohung für eine Organisation
  - 2.4 Die Wahrscheinlichkeit größerer Cyber-Angriffe
  - 2.5 Black Swan events

3. Modellierung von Bedrohungen
  - 3.1 Methodik des Angriffsbaumes
  - 3.2 STRIDE
  - 3.3 DREAD
  - 3.4 Schmerzpyramide – “Pyramid of Pain”
4. Bibliotheken angreifen
  - 4.1 CAPEC
  - 4.2 Soloves Taxonomie der Privatsphäre
  - 4.3 Modellierung mit Mitre ATT&CK®
  - 4.4 Identifizierung neuer Arten von Angriffen
5. Regeln, Vorschriften und Strafverfolgung
  - 5.1 Cyber-Gesetze
  - 5.2 Compliance und Strafverfolgung
6. Risiko-Management
  - 6.1 Veränderte Herangehensweisen an das Risikomanagement
  - 6.2 Reaktion auf Zwischenfälle und Krisenmanagement
  - 6.3 Berücksichtigung der Black Swan Events
  - 6.4 Kontinuierliche Neubewertung
7. Threat Mitigation
  - 7.1 Defensive Taktiken und Technologien
  - 7.2 Strategien zur Risikominderung
  - 7.3 Validierung des Abwehrschutzes
  - 7.4 Sicherheit und Privacy by Design
  - 7.5 Implementierung von Mechanismen zur Verminderung der Bedrohungen in einer Organisation



**Literatur****Pflichtliteratur****Weiterführende Literatur**

- CAPEC: Common Attack Pattern Enumeration and Classification. <https://capec.mitre.org/>
- Kim, P. (2014): The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC.
- Kim, P. (2015): The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC.
- Kim, P. (2018): The Hacker Playbook 3: Practical Guide to Penetration Testing. Secure Planet LLC.
- Mitre ATT&CK®. <https://attack.mitre.org/>
- Pfleeger, C. P. / Pfleeger, S. L. / Margulies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

# Projekt: Threat Modeling

Kurscode: DLBCSEEF202\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01; DLBCSEEF201_D oder DLBCSEEF201_E

## Beschreibung des Kurses

Die Bedrohungen für moderne Computersysteme sind vielfältig und entwickeln sich ständig weiter. In diesem Projekt hat der Studierende die Gelegenheit, die Kunst und Wissenschaft der Bedrohungsmodellierung auf ein Szenario anzuwenden, das vom Dozenten zusammen mit dem Studierenden definiert wird. Die Grundlage bilden reale oder fiktive Fallstudien, zu denen der Studierende unter Verwendung einer geeigneten Methodik die Bedrohungen identifizieren und darüber berichten soll. Diese kann aus Methoden wie Attack Trees, STRIDE, DREAD oder einer gerechtfertigten Aufzählung von CAPEC oder Mitre ATT&CK® TTPs ausgewählt werden, je nachdem, was der Kursteilnehmer für am geeignetsten hält. Die Ergebnisse werden in Form eines Berichts präsentiert.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihr Wissen über die Modellierung von Bedrohungen auf Fälle und Szenarien anzuwenden.
- ihr daraus resultierendes Modell auf der Grundlage einer soliden Argumentation und in Bezug auf bekannte Techniken, Taktiken und Verfahren der Angreifer zu rechtfertigen.
- einen Bericht zu verfassen, der ihre Argumentation in systematischer und verständlicher Weise darlegt.

## Kursinhalt

- Für einen bestimmten Fall oder ein bestimmtes Szenario modellieren Studierende die Bedrohungen unter Verwendung einer etablierten Methodik und reicht dann den Bericht und, falls zutreffend, alle Codes und Daten ein. Spezifische Probleme und Kontexte werden vom Tutor vorgegeben, Vorschläge der Studierenden können jedoch berücksichtigt werden.

**Literatur**

**Pflichtliteratur**

**Weiterführende Literatur**

- Case Studies (Cyber): <https://www.securitymagazine.com/topics/2664-case-studies-cyber>
- Karger, P. A. / Scherr, R. R. (1974): MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS.
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 40 (3):769.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.
- Van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

DLBCSEEF02\_D

## Cloud Security

Module Code: DLBCSEECs\_E

<b>Module Type</b> see curriculum	<b>Admission Requirements</b> <ul style="list-style-type: none"> <li>▪ DLBDSCC01 or DLBDSCC01_D</li> <li>▪ DLBDSCC01 or DLBDSCC01_D, DLBCSEECs01_E</li> </ul>	<b>Study Level</b> BA	<b>CP</b> 10	<b>Student Workload</b> 300 h
--------------------------------------	---	--------------------------	-----------------	----------------------------------

<b>Semester / Term</b> see curriculum	<b>Duration</b> Minimum 1 semester	<b>Regularly offered in</b> WiSe/SoSe	<b>Language of Instruction and Examination</b> English
--	--	--	---

### Module Coordinator

Prof. Dr. Ahmed Taha (Security Controls in the Cloud) / N.N. (Project: Security by Design in the Cloud)

### Contributing Courses to Module

- Security Controls in the Cloud (DLBCSEECs01\_E)
- Project: Security by Design in the Cloud (DLBCSEECs02\_E)

### Module Exam Type

#### Module Exam

#### Split Exam

##### Security Controls in the Cloud

- Study Format "Distance Learning": Exam, 90 Minutes

##### Project: Security by Design in the Cloud

- Study Format "Distance Learning": Written Assessment: Project Report

### Weight of Module

see curriculum

<p><b>Module Contents</b></p> <p><b>Security Controls in the Cloud</b></p> <ul style="list-style-type: none"> <li>▪ Cloud security</li> <li>▪ Losing the intranet</li> <li>▪ Security by design</li> <li>▪ Secure cloud coding</li> <li>▪ Confidentiality aspects</li> <li>▪ Monitoring and Audit</li> </ul> <p><b>Project: Security by Design in the Cloud</b></p> <p>This module is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.</p>	
<p><b>Learning Outcomes</b></p> <p><b>Security Controls in the Cloud</b></p> <p>On successful completion, students will be able to</p> <ul style="list-style-type: none"> <li>▪ design a secure cloud deployment using infrastructure as code methodologies.</li> <li>▪ understand cloud-specific attacks and threat models.</li> <li>▪ define appropriate storage classes in compliance with security requirements.</li> <li>▪ monitor cloud resources to detect misuse and incidents.</li> </ul> <p><b>Project: Security by Design in the Cloud</b></p> <p>On successful completion, students will be able to</p> <ul style="list-style-type: none"> <li>▪ transfer previously acquired knowledge about cloud security to practical use cases.</li> <li>▪ design, architect, and implement a working cloud-based system.</li> <li>▪ reason about design choices of and how best cloud security practices are followed.</li> <li>▪ critically evaluate said choices with respect to the stated design goal.</li> <li>▪ describe and explain the resulting solution in a report.</li> </ul>	
<p><b>Links to other Modules within the Study Program</b></p> <p>This module is similar to other modules in the fields of Computer Science &amp; Software Development</p>	<p><b>Links to other Study Programs of the University</b></p> <p>All Bachelor Programs in the IT &amp; Technology fields</p>



## Security Controls in the Cloud

Course Code: DLBCSE ECS01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D

### Course Description

Maintaining a datacenter is expensive and inflexible, so it is expected that most corporations will be moving their server-based processes to a private, public or hybrid cloud in the next few years. Doing so will make operations more flexible and elastic but poses challenges to security architectures and operations. The paradigm of Infrastructure as Code (IaC) has been embraced by cloud providers and is a great opportunity to architect security into the design of a system (security by design) utilizing security best practices. However, too often, we see the on-premises mentality being applied to cloud deployments resulting in less secure systems instead of utilizing the security advantages a cloud provides. This course teaches the principles of Cloud Native security and how to avoid common pitfalls.

### Course Outcomes

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

### Contents

1. Cloud security is different
  - 1.1 Shared responsibility model
  - 1.2 Infrastructure as code
  - 1.3 The Private, Public and Hybrid Cloud
  - 1.4 Types of virtualization
  - 1.5 Cloud threat models: Mitre Cloud ATT&CK
2. Losing the intranet
  - 2.1 Identify and Access Management
  - 2.2 Principle of least privilege and fine-grained cloud access control
  - 2.3 Using Software Defined Networks, virtual private clouds and subnets
  - 2.4 Moving to a serverless architecture
  - 2.5 Defense in depth

3. Security by design
  - 3.1 Orchestration: Infrastructure as Code
  - 3.2 The Automate-Everything principle, Updating and Repeatability
  - 3.3 Reuse of good design patterns
  - 3.4 Container security
  - 3.5 Identification and Authentication
4. Secure cloud coding
  - 4.1 Software supply chain security
  - 4.2 Continuous Integration and Deployment
  - 4.3 Testing in code integration for security
  - 4.4 Canaries in code deployment
  - 4.5 Policy engines
5. Confidentiality aspects
  - 5.1 Secrets management
  - 5.2 Encryption of data at rest
  - 5.3 Encryption of data in transit
  - 5.4 Data leakage and exfiltration
6. Availability
  - 6.1 Storage tiers and locality
  - 6.2 Backup strategies
  - 6.3 Data and process redundancy
  - 6.4 Data lifecycle configuration
  - 6.5 DDoS mitigation
7. Locality
  - 7.1 Compliance requirements
  - 7.2 Geography of data/processes
  - 7.3 Redundancy of data centers
  - 7.4 Colocation for performance reasons
8. Monitoring and Audit
  - 8.1 Centralized logging
  - 8.2 Auditing orchestration scripts
  - 8.3 Detecting misconfigurations
  - 8.4 Cloud Forensics

9. Summary and Research topics
  - 9.1 Homomorphic encryption
  - 9.2 Attestation
  - 9.3 Proof-carrying data
  - 9.4 Side-channel attacks
  - 9.5 Conclusions

**Literature****Compulsory Reading****Further Reading**

- Mitre Cloud ATT&CK. <https://attack.mitre.org/matrices/enterprise/cloud/>

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides

## Project: Security by Design in the Cloud

Course Code: DLBCSE ECS02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSE ECS01_E

### Course Description

This course provides the opportunity to implement a cloud software system using best cloud security practices. A list of ideas is provided on the online learning platform. In addition, the students can contribute use case ideas of their own after consulting with the tutor. The core aim is to apply the theoretical knowledge of cloud security methods and best practices to implement an application that is deployed as an Infrastructure-as-code project, can be monitored and audited, as well as easily and preferably automatically updated without danger. This entails reasoning about possible design and architectural choices in a rational way, as well as implementing them on a cloud platform, such as CNCF, Amazon AWS, Microsoft Azure or Google GCP.

### Course Outcomes

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

### Contents

- This course is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

### Literature

#### Compulsory Reading

#### Further Reading

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Project
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Project Report

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides

# Pentesting

Module Code: DLBCSEPT\_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	<ul style="list-style-type: none"> <li>▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D</li> <li>▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEPT01_E</li> </ul>	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

## Module Coordinator

Enno Nagel (Principles of Ethical Hacking) / N.N. (Project: Pentesting)

## Contributing Courses to Module

- Principles of Ethical Hacking (DLBCSEPT01\_E)
- Project: Pentesting (DLBCSEPT02\_E)

## Module Exam Type

### Module Exam

### Split Exam

#### Principles of Ethical Hacking

- Study Format "Distance Learning": Exam, 90 Minutes

#### Project: Pentesting

- Study Format "Distance Learning": Written Assessment: Project Report

<p><b>Weight of Module</b> see curriculum</p>	
<p><b>Module Contents</b></p> <p><b>Principles of Ethical Hacking</b></p> <ul style="list-style-type: none"> <li>▪ Introduction to Ethical Hacking</li> <li>▪ Reconnaissance</li> <li>▪ Enumeration and Vulnerability Analysis</li> <li>▪ Hacking Systems</li> <li>▪ Malware</li> </ul> <p><b>Project: Pentesting</b></p> <p>In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system.</p>	
<p><b>Learning Outcomes</b></p> <p><b>Principles of Ethical Hacking</b></p> <p>On successful completion, students will be able to</p> <ul style="list-style-type: none"> <li>▪ understand the concepts, ethical and legal frameworks for penetration testing activity.</li> <li>▪ plan a penetration testing campaign.</li> <li>▪ use the tools and methods to execute the plan.</li> <li>▪ organize a bug bounty program and work with penetration testers.</li> <li>▪ write reports for the target audience.</li> </ul> <p><b>Project: Pentesting</b></p> <p>On successful completion, students will be able to</p> <ul style="list-style-type: none"> <li>▪ execute a successful penetration test.</li> <li>▪ write appropriate reports.</li> </ul>	
<p><b>Links to other Modules within the Study Program</b></p> <p>This module is similar to other modules in the fields of Computer Science &amp; Software Development</p>	<p><b>Links to other Study Programs of the University</b></p> <p>All Bachelor Programs in the IT &amp; Technology fields</p>



# Principles of Ethical Hacking

Course Code: DLBCSEPT01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D

## Course Description

Ethical hacking is an essential part in testing security implementations as well as discovering overlooked security issues. In this course, we will look at the principles and tools that hackers use and how ethical hacking is effectively utilized.

## Course Outcomes

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

## Contents

1. Introduction to Ethical Hacking
  - 1.1 Overview of Cyber Security
  - 1.2 Concepts of Cyber Kill Chain
  - 1.3 Hacking vs Ethical Hacking
  - 1.4 Laws and Standards
2. Reconnaissance
  - 2.1 Footprinting Techniques
  - 2.2 Network Scanning
  - 2.3 Host Discovery
  - 2.4 Service, Port and OS Discovery
  - 2.5 Scan beyond Security Measures

3. Enumeration and Vulnerability Analysis
  - 3.1 Enumeration Techniques
  - 3.2 Enumeration Countermeasures
  - 3.3 Vulnerability Assessment Techniques
  - 3.4 Vulnerability Classification and Assessment
4. Hacking Systems
  - 4.1 Gaining Access to Systems
  - 4.2 Privilege Escalation
  - 4.3 Persistent Access
  - 4.4 Covering Traces
5. Malware
  - 5.1 Types of Malware
  - 5.2 Concepts of Fileless Malware
  - 5.3 Countermeasures
6. Sniffing
  - 6.1 Concepts of Sniffing
  - 6.2 Sniffing Techniques
  - 6.3 Countermeasures
7. Denial of Service
  - 7.1 Concepts of DoS/DDoS
  - 7.2 Attack Techniques
  - 7.3 Botnets
  - 7.4 Countermeasures
8. Social Engineering
  - 8.1 Concepts of Social Engineering
  - 8.2 Social Engineering Techniques
  - 8.3 Identity Theft and Impersonation
  - 8.4 Countermeasures

**Literature****Compulsory Reading****Further Reading**

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: <https://www.acsac.org/2002/papers/classic-multics-orig.pdf> [last accessed: 25 August 2020]).
- Mitre PreATT&CK. <https://attack.mitre.org/matrices/pre/>
- Mitre Enterprise ATT&CK. <https://attack.mitre.org/matrices/enterprise/>
- Mitre Mobile ATT&CK. <https://attack.mitre.org/matrices/mobile/>
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. <https://github.com/blaCkHatHacEEkr/PENTESTING-BIBLE>

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides

## Project: Pentesting

Course Code: DLBCSEPT02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEPT01_E

### Course Description

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system. Students write a report outlining the vulnerabilities found, the methods used and proposals for fixing that class of vulnerability.

### Course Outcomes

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

### Contents

- The student will be provided with virtual environments emulating corporate systems and an attacker machine with the necessary tools.

### Literature

#### Compulsory Reading

#### Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: <https://www.acsac.org/2002/papers/classic-multics-orig.pdf> [last accessed: 25 August 2020]).
- Mitre PreATT&CK. <https://attack.mitre.org/matrices/pre/>
- Mitre Enterprise ATT&CK. <https://attack.mitre.org/matrices/enterprise/>
- Mitre Mobile ATT&CK. <https://attack.mitre.org/matrices/mobile/>
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. <https://github.com/blaCkHatHacEEkr/PENTESTING-BIBLE>

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Project
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Project Report

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides

# Industrielle Systemsicherheit

Modulcode: DLBCSEEIST\_D

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ DLBINGEIT01 oder DLBINGEIT01_E</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	---	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Marian Benner-Wickner (Grundlagen der industriellen Softwaretechnik) / N.N. (Sicherheit im Internet of Things)

## Kurse im Modul

- Grundlagen der industriellen Softwaretechnik (IGIS01)
- Sicherheit im Internet of Things (DLBCSEEIST01\_D)

## Art der Prüfung(en)

<b>Modulprüfung</b>	<b>Teilmodulprüfung</b> <u>Grundlagen der industriellen Softwaretechnik</u> <ul style="list-style-type: none"> <li>• Studienformat "Kombistudium": <i>Prüfungsart</i></li> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> <li>• Studienformat "myStudium": <i>Prüfungsart</i></li> </ul> <u>Sicherheit im Internet of Things</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> </ul>
---------------------	---

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****Grundlagen der industriellen Softwaretechnik**

- Aufbau und Organisation von Informationssystemen
- Risiken und Herausforderungen der industriellen Softwaretechnik
- Softwarelebenszyklus: Von Planung bis Ablösung
- Requirements Engineering und Spezifikation
- Architektur und Implementierung
- Qualitätssicherung, Betrieb und Weiterentwicklung
- Rollen im Software Engineering
- Organisation von Softwareprojekten
- Softwareprozessmodell-Rahmenwerke

**Sicherheit im Internet of Things**

- Grundlagen des Internet der Dinge (IoT)
- Angriffe auf das Internet der Dinge
- Sicherheit durch Design
- Sichern von Geräten für das Internet der Dinge
- Operative Sicherheit
- Cloud-Sicherheit
- Große Daten / Künstliche Intelligenz

**Qualifikationsziele des Moduls****Grundlagen der industriellen Softwaretechnik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einfache Berechnungen im Binärsystem (Boolsche Algebra) durchzuführen.
- den Aufbau von Rechnersystemen und Kommunikationsnetzen zu beschreiben.
- die Phasen eines SW-Lebenszyklus voneinander abzugrenzen.
- Rollen und Phasen im Software-Prozess voneinander abzugrenzen.
- verschiedene Vorgehensmodelle der SW-Entwicklung zu kennen.
- typische Herausforderungen und Risiken der industriellen SW-Entwicklung zu kennen.
- verschiedene Programmierparadigmen und deren Einsatz zu kennen.

**Sicherheit im Internet of Things**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte von IoT-Architekturen zu kennen und zu verstehen.
- die gängigsten Schwachstellen, Bedrohungen und Risiken für das Internet der Dinge zu kennen und zu verstehen.
- Gegenmaßnahmen für IoT-Schwachstellen zu verstehen und anzuwenden.
- ein IoT-Architekturmodell/eine IoT-Lösung zu analysieren.



**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Grundlagen der industriellen Softwaretechnik

Kurscode: IGIS01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen Einblick in die technischen und theoretischen Grundlagen des Software Engineering zu vermitteln. Neben dem generellen Aufbau von Rechnersystemen werden den Studierenden typische Herausforderungen bei der Entwicklung industrieller Informationssysteme vermittelt. Darüber hinaus wird dargestellt, mit welchen typischen Phasen und Aktivitäten im Software Engineering diese Risiken gezielt adressiert werden.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einfache Berechnungen im Binärsystem (Boolsche Algebra) durchzuführen.
- den Aufbau von Rechnersystemen und Kommunikationsnetzen zu beschreiben.
- die Phasen eines SW-Lebenszyklus voneinander abzugrenzen.
- Rollen und Phasen im Software-Prozess voneinander abzugrenzen.
- verschiedene Vorgehensmodelle der SW-Entwicklung zu kennen.
- typische Herausforderungen und Risiken der industriellen SW-Entwicklung zu kennen.
- verschiedene Programmierparadigmen und deren Einsatz zu kennen.

## Kursinhalt

1. Aufbau und Organisation von Informationssystemen
  - 1.1 0 und 1 als Grundlage aller IT-Systeme
  - 1.2 Von-Neumann-Architektur
  - 1.3 Verteilte Systeme und Kommunikationsnetze
  - 1.4 Betriebliche Informationssysteme
2. Risiken und Herausforderungen der industriellen Softwaretechnik
  - 2.1 Eigenschaften von industriellen Softwaresystemen
  - 2.2 Softwaretechnik
  - 2.3 Risiken und typische Probleme
  - 2.4 Ursachenforschung
  - 2.5 Herausforderungen im Software Engineering

3. Softwarelebenszyklus: Von Planung bis Ablösung
  - 3.1 Der Softwarelebenszyklus im Überblick
  - 3.2 Planung
  - 3.3 Entwicklung
  - 3.4 Betrieb
  - 3.5 Wartung
  - 3.6 Abschaltung
4. Requirements Engineering und Spezifikation
  - 4.1 Requirements Engineering
  - 4.2 Spezifikation
5. Architektur und Implementierung
  - 5.1 Architektur
  - 5.2 Implementierung
6. Qualitätssicherung, Betrieb und Weiterentwicklung
  - 6.1 Qualitätssicherung
  - 6.2 Betrieb
  - 6.3 Weiterentwicklung
7. Rollen im Software Engineering
  - 7.1 Idee der rollenbasierten Herangehensweise
  - 7.2 Typische Rollen
8. Organisation von Softwareprojekten
  - 8.1 Vom Prozessparadigma zum Softwareprozess
  - 8.2 Prozessparadigmen
9. Softwareprozessmodell-Rahmenwerke
  - 9.1 V-Modell XT
  - 9.2 Rational Unified Process (RUP)
  - 9.3 Scrum

**Literatur**

**Pflichtliteratur**

**Weiterführende Literatur**

- Gumm, H. P./Sommer, M. (2011): Einführung in die Informatik. 9. Auflage, Oldenbourg, München.
- Hansen, H. R./Neumann, G. (2009): Wirtschaftsinformatik 1. Grundlagen und Anwendungen. 10. Auflage, UTB, Stuttgart.
- Ludewig, J./Lichter, H. (2010): Software Engineering. Grundlagen, Menschen, Prozesse, Techniken. 2. Auflage, dpunkt.verlag, Heidelberg.
- Sommerville, I. (2007): Software Engineering. 8. Auflage, Addison-Wesley, Boston.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b>
------------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b>
---------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

# Sicherheit im Internet of Things

Kurscode: DLBCSEEIST01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBINGEIT01 oder DLBINGEIT01_E

## Beschreibung des Kurses

Das Internet der Dinge (IoT) ist ein Megatrend. Er umfasst sowohl Endverbrauchersysteme als auch industrielle Systeme und Technologien (Industrial IoT, oder IIoT). Es gibt eine zunehmende Anzahl miteinander verbundener Geräte, aus denen sich das Internet der Dinge zusammensetzt. Im Allgemeinen besteht die Architektur des Internet der Dinge aus Endgeräten, Cloud-Lösungen und Akteuren/Sensoren. Die Sicherheit des Internet der Dinge bringt verschiedene Themen zusammen, d.h. Netzwerkprotokolle, Software, Hardware, Kryptographie und Cloud Computing.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte von IoT-Architekturen zu kennen und zu verstehen.
- die gängigsten Schwachstellen, Bedrohungen und Risiken für das Internet der Dinge zu kennen und zu verstehen.
- Gegenmaßnahmen für IoT-Schwachstellen zu verstehen und anzuwenden.
- ein IoT-Architekturmodell/eine IoT-Lösung zu analysieren.

## Kursinhalt

1. Grundlagen des Internet der Dinge (IoT)
  - 1.1 Einführung
  - 1.2 Architektur
  - 1.3 Nicht-industrielles Internet der Dinge
  - 1.4 Industrie 4.0 (Industrielles IoT)
2. Angriffe auf das Internet der Dinge
  - 2.1 Verwundbarkeiten, Bedrohungen und Risiken
  - 2.2 Cyber-Angriffe und Gegenmaßnahmen
3. Sicherheit durch Design
  - 3.1 Projektmanagement / Sicherer Lebenszyklus der Entwicklung
  - 3.2 Statische Prüfung
  - 3.3 Dynamische Prüfung
  - 3.4 DevSecOps



4. Sichern von Geräten für das Internet der Dinge
  - 4.1 Sicherheitsrisiken
  - 4.2 Entwurfsziele
5. Operative Sicherheit
  - 5.1 Informations- und Cyber-Sicherheitsverwaltungssystem
  - 5.2 Netzwerk-Sicherheit
  - 5.3 Gerätekonfiguration
  - 5.4 Authentifizierung und Autorisierung
6. Cloud-Sicherheit
  - 6.1 Konzept des Nebels
  - 6.2 Bedrohungen für Cloud Internet of Things-Dienste
  - 6.3 Cloudbasierte Sicherheitsdienste
  - 6.4 Sichern der Cloud-Lösung
7. Big Data / Künstliche Intelligenz
  - 7.1 Beaufsichtigtes Lernen
  - 7.2 Unbeaufsichtigtes Lernen

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Butun, I. (2020): Industrial IoT. Challenges, Design Principles, Applications, and Security. 1st Edition, Springer International Publishing, Cham.
- Gupta B./Quamara, M. (2020): Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. 1st edition, CRC Press, Boca Raton, FL.
- Liyanage, M. et al. (2020): IoT Security. Advances in Authentication. 1st edition, John Wiley & Sons Ltd., Hoboken, NJ.
- Russell, B./Van Duren, D. (2018): Practical Internet of Things Security. Design a security framework for an Internet connected ecosystem. 2nd edition, Packt Publishing Ltd., Birmingham.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# Cyber Threat Intelligence

Module Code: DLBCSEECTI\_E

<b>Module Type</b> see curriculum	<b>Admission Requirements</b> <ul style="list-style-type: none"> <li>▪ none</li> <li>▪ DLBCSEECTI01_E</li> </ul>	<b>Study Level</b> BA	<b>CP</b> 10	<b>Student Workload</b> 300 h
--------------------------------------	--	--------------------------	-----------------	----------------------------------

<b>Semester / Term</b> see curriculum	<b>Duration</b>	<b>Regularly offered in</b> WiSe/SoSe	<b>Language of Instruction and Examination</b> English
--	-----------------	--	---

## Module Coordinator

Dr. Christian Prause (Attack Models and Threat Feeds) / N.N. (Project: Defense against APTs)

## Contributing Courses to Module

- Attack Models and Threat Feeds (DLBCSEECTI01\_E)
- Project: Defense against APTs (DLBCSEECTI02\_E)

## Module Exam Type

### Module Exam

### Split Exam

Attack Models and Threat Feeds

- Study Format "Distance Learning": Exam, 90 Minutes

Project: Defense against APTs

- Study Format "Distance Learning": Written Assessment: Project Report

## Weight of Module

see curriculum

**Module Contents****Attack Models and Threat Feeds**

- Threat actors
- Modeling an Attack
- Attack Preparation TTPs
- Enterprise TTPs
- Industrial Control Systems TTPs
- Reporting

**Project: Defense against APTs**

Using well-known methods like the MITRE ATT&CK Techniques, Tactics and Procedures students will be able to produce a comprehensive threat model. Therefore, students will have to determine through simulation or a “table top exercise” which data is already available and which external threat feed data is required. After analyzing the “attack side” students will utilize threat intelligence systems for diagnostic to do a gap analysis – especially what defense technology is missing – and will be able to give sound advice to enhance resilience and to foster response capabilities. Emphasis will be drawn on the practical aspects of the defense against a given threat actor using techniques including beyond technical solutions and determine what cooperation with CERTs and ISPs is required to effectively defend against threats.

**Learning Outcomes****Attack Models and Threat Feeds**

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

**Project: Defense against APTs**

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT’s, ISP’s and IT-Security companies.

**Links to other Modules within the Study Program**

This module is similar to other modules in the fields of Computer Science & Software Development

**Links to other Study Programs of the University**

All Bachelor Programs in the IT & Technology fields

## Attack Models and Threat Feeds

Course Code: DLBCSEECTI01\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

### Course Description

In this course, we look in depth at modeling threats and using data to diagnose, analyze and make recommendations. After a broad look at threat actors, we look at a variety of ways of modeling threats. This spans from Attack Trees to Kill Chains, but whichever method works the best, it all boils down to adversary Techniques, Tactics and Procedures. We look into the various taxonomies of these as defined by Mitre's ATT&CK and determine what can be observed in data. It is rare that internal data is enough for a complete analysis and in practice the threat analyst must use external data sources. These are available in a variety of formats, but the industry is converging on STIX and the use of software platforms like ACT to do the parsing and provide a good user experience. After looking at examples of threat actors and reports on them, we tackle the problem of making recommendations and writing reports. In some cases, engaging with law enforcement is required in which case some particularities need to be observed.

### Course Outcomes

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

### Contents

1. Threat Actors
  - 1.1 Script Kiddies
  - 1.2 eCrime Threat Actors
  - 1.3 Advanced Persistent Threat Actors (APT)
  - 1.4 Threat Researchers
2. Modeling an Attack
  - 2.1 Phases of an Attack
  - 2.2 Lockheed Martin Kill-Chain
  - 2.3 Attack Trees
  - 2.4 Models for Security Risks and Cyber Attacks

3. Attack preparation TTPs
  - 3.1 Observability of Attack Preparations
  - 3.2 Operational Security of an Organization
4. Enterprise TTPs
  - 4.1 Behaviors of the Attacker
  - 4.2 Observable Data in an Enterprise
5. Industrial Control Systems TTPs
  - 5.1 Critical Infrastructure
  - 5.2 Special Considerations with IoT/ICS Defense
6. Threat data exchange
  - 6.1 Indicators of Compromise vs. Indicators of Attack
  - 6.2 Threat Intelligence Reports
  - 6.3 Ad-hoc Data Formats
  - 6.4 STIX Format, TAXII Protocol
  - 6.5 Semantics of Threat Data using Mitre ATT&CK, CVEs, etc.
7. Examples of Threat Analysis Platforms
  - 7.1 ACT Platform
  - 7.2 MISP
  - 7.3 OpenCTI
8. Examples of Threat Actors and their Modus Operandi
  - 8.1 Threat Model
  - 8.2 Relevant Indicator Data
  - 8.3 Relevant CTI Data
  - 8.4 Diagnosing the Threat
  - 8.5 Data Coverage Gap Analysis
9. Reporting
  - 9.1 Mapping Raw Data to Mitre ATT&CK
  - 9.2 Making Defensive Recommendations
  - 9.3 Writing Reports for Technical Staff
  - 9.4 Writing Reports for Management
  - 9.5 Working with Law Enforcement

**Literature****Compulsory Reading****Further Reading**

- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: <https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LMWhite-Paper-Intel-Driven-Defense.pdf>)
- MISP Platform: <https://www.misp-project.org/>
- Mitre ATT&CK. <https://attack.mitre.org/>
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.



**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Online Lecture
--	--------------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> yes
<b>Type of Exam</b>	Exam, 90 Minutes

<b>Student Workload</b>					
<b>Self Study</b>	<b>Contact Hours</b>	<b>Tutorial</b>	<b>Self Test</b>	<b>Independent Study</b>	<b>Hours Total</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input type="checkbox"/> Guideline <input checked="" type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Slides

## Project: Defense against APTs

Course Code: DLBCSEECTI02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEECTI01_E

### Course Description

This project course will give students hands-on experience in the challenging task to analyze threat vectors and real attacks of highly sophisticated, well planned, prepared and conducted attack campaigns named “Advanced Persistent Threats – APT’s” which derive from state, non-state or highly criminal attackers. Students will need to consider all practical aspects of different attack vectors using technical and non-technical (like social engineering) methods and procedures. To have the right understanding how to defend against these attacks they will use an attack simulator like Foreseeti SecureCAD or AttackIQ or conduct a “table top exercise” to figure out what data is required to analyze what security components and system configurations are needed to defend against a given, highly capable threat actor. Through this course, students will develop a complete overview what technical applications can be used to enhance resilience, foster response capabilities and recover from such attacks. Furthermore, students will have to take into account so called “soft measures” like organizational and procedural policies and regulations, bearing in mind the human factor in its social and psychological form. Through the cooperation with CERT’s, ISP’s and IT-Security Companies, academics and state agencies, students will cooperate on international level with IT-experts and experts from other disciplines to improve their expertise and to develop their personality.

### Course Outcomes

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT’s, ISP’s and IT-Security companies.

### Contents

- This project course focuses on practical aspects how to defend against APTs. Students will start with a given use case to analyze a real-world APT Attack against a defined IT-System / Network, identify the different attack vectors on multiple levels and make the necessary data regarding used malware and exploits, techniques and procedures available by using a simulator or conducting a “table top exercise”. With this, students will develop a

comprehensive picture of vulnerabilities and security shortfalls in the IT-system / network of their own enterprise. Students will then have to analyze and identify what technical or non-technical measures could have prevented this attack using an interdisciplinary approach taking all levels and involved actors into account. Cooperation with other national and international CERT's, ISP, IT-Security companies and state agencies will be the basis for a sound assessment how to improve the own resilience using best practices, state of the art technologies and considering new technologies.

- All relevant artifacts and considerations are documented by the students in a comprehensive project report.

## Literature

### Compulsory Reading

### Further Reading

- ACT Platform: <https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/>
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: <https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>)
- MISP Platform: <https://www.misp-project.org/>
- Mitre PreATT&CK. <https://attack.mitre.org/matrices/pre/>
- Mitre Enterprise ATT&CK. <https://attack.mitre.org/matrices/enterprise/>
- Mitre Mobile ATT&CK. <https://attack.mitre.org/matrices/mobile/>
- Mitre ICS ATT&CK: [https://collaborate.mitre.org/attackics/index.php/Main\\_Page](https://collaborate.mitre.org/attackics/index.php/Main_Page)
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: <https://github.com/OpenCTI-Platform/opencti>
- Semantics of threat data: <http://www.ti-semantic.com>
- STIX: <https://www.oasis-open.org/standards#stix2.1>
- TAXII: <https://www.oasis-open.org/standards#taxii2.1>
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. <https://zeltser.com/cyber-threat-intel-and-ir-report-template/>

**Study Format Distance Learning**

<b>Study Format</b> Distance Learning	<b>Course Type</b> Project
--	-------------------------------

<b>Information about the examination</b>	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no
<b>Type of Exam</b>	Written Assessment: Project Report

<b>Student Workload</b>					
<b>Self Study</b> 120 h	<b>Contact Hours</b> 0 h	<b>Tutorial</b> 30 h	<b>Self Test</b> 0 h	<b>Independent Study</b> 0 h	<b>Hours Total</b> 150 h

<b>Instructional Methods</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides

# Telekommunikationspezifische Bedrohungen

Modulcode: DLBCSEEMT\_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	<ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ DLBIBRVS01 oder DLBIBRVS01_E;</li> <li>▪ DLBCSEINF01_D oder DLBCSEINF01_E</li> </ul>	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

N.N. (Funk- und Telekommunikationssicherheit) / N.N. (Softwarearchitektur mobiler Geräte)

## Kurse im Modul

- Funk- und Telekommunikationssicherheit (DLBCSEEMT01\_D)
- Softwarearchitektur mobiler Geräte (DLBCSEEMT02\_D)

## Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	<p><u>Funk- und Telekommunikationssicherheit</u></p> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> </ul> <p><u>Softwarearchitektur mobiler Geräte</u></p> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur, 90 Minuten</li> </ul>
<p><b>Anteil der Modulnote an der Gesamtnote</b></p> <p>s. Curriculum</p>	

**Lehrinhalt des Moduls****Funk- und Telekommunikationssicherheit**

- Überblick über drahtlose Protokolle
- Grundlagen von Drahtlosen Netzwerken
- Telekommunikationsprotokoll-Klassen
- Telekom-Architektur
- Sicherheit von Handapparaten und Geräten
- Bedrohungen
- Andere drahtlose Anwendungen
- Schutzmaßnahmen

**Softwarearchitektur mobiler Geräte**

- Mobil-Technologie-Stacks
- Hardware
- Android-Betriebssystem
- Apple iOS-Betriebssystem
- Mobile Geräte
- Software-Ökosysteme und Sicherheit
- Bedrohungen von Mobiltelefone
- Verwaltung mobiler Geräte

**Qualifikationsziele des Moduls****Funk- und Telekommunikationssicherheit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen der bei der Datenübertragung verwendeten drahtlosen Signale zu verstehen.
- verschiedene Arten der drahtlosen Vernetzung zu identifizieren und ihre Unterschiede zu verstehen.
- Telekommunikationsterminologie zu verstehen und diese der IT-Terminologie gegenüberzustellen.
- Architekturen der wichtigsten drahtlosen Telekommunikationssysteme zu verstehen.
- Angriffsvektoren gegen mobile Geräte sowie das Kernnetzwerk zu verstehen.
- andere Arten der Vernetzung, die möglicherweise genutzt werden, zu finden.

**Softwarearchitektur mobiler Geräte**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Hardware- und Software-Stacks gängiger Mobiltelefone zu verstehen.
- die Sicherheitskontrollen in diesen Stacks verstehen.
- zu erkennen, welche Schutzmaßnahmen und Risiken mit den Ökosystemen der Geräte verbunden sind.
- zu erkennen, welche Angriffe in der Vergangenheit erfolgreich waren.
- die Verwaltung mobiler Endgeräte zum Schutz eines Unternehmens zu nutzen.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor -Programme im Bereich IT & Technik

# Funk- und Telekommunikationssicherheit

Kurscode: DLBCSEEMT01\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch	-1	5	DLBIBRVS01 oder DLBIBRVS01_E; DLBCSEINF01_D oder DLBCSEINF01_E

## Beschreibung des Kurses

Die Zahl der Geräte, die drahtlos mit Netzwerken verbunden werden können, hat bereits die Zahl der Desktop- und Laptop-Computer überholt, die über ein Kabel mit einem lokalen Netzwerk verbunden sind. Vor allem Telefone und Tablets dominieren den Markt, die sich mit den drahtlosen Telekommunikationsnetzen verbinden. Es gibt aber auch viele andere Formen der drahtlosen Kommunikation, die von Geräten genutzt werden. Die Eigenheiten dieser drahtlosen Systeme müssen verstanden werden, um sie in ein vollständiges Sicherheitskonzept zu integrieren. Drahtlose Protokolle zwingen den User oft dazu, einem System zu vertrauen, in das er keinen Einblick hat. In diesem Kurs widmen wir uns genau diesem Thema.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen der bei der Datenübertragung verwendeten drahtlosen Signale zu verstehen.
- verschiedene Arten der drahtlosen Vernetzung zu identifizieren und ihre Unterschiede zu verstehen.
- Telekommunikationsterminologie zu verstehen und diese der IT-Terminologie gegenüberzustellen.
- Architekturen der wichtigsten drahtlosen Telekommunikationssysteme zu verstehen.
- Angriffsvektoren gegen mobile Geräte sowie das Kernnetzwerk zu verstehen.
- andere Arten der Vernetzung, die möglicherweise genutzt werden, zu finden.

## Kursinhalt

1. Überblick über drahtlose Protokolle
  - 1.1 Netzwerkprotokolle für den persönlichen Bereich (Bluetooth, RFID, NFC und andere)
  - 1.2 Protokolle für drahtlose lokale Netzwerke (802.11a,b, g, ac , p und weitere)
  - 1.3 Wide Area Network-Protokolle (Telekommunikationsprotokolle, LoRa, Satellitenprotokolle und mehr)
  - 1.4 Schlüsselaustausch und Kryptographie in drahtlosen Netzwerken



2. Grundlagen von Drahtlosen Netzwerken
  - 2.1 Frequenzen
  - 2.2 Modulationen
  - 2.3 Daten-Kodierungen
  - 2.4 Zielkonflikte
3. Telekommunikationsprotokoll-Klassen
  - 3.1 Telekommunikation vs. IT-Terminologie und -Technologien
  - 3.2 Telekommunikationsnormen
  - 3.3 Veraltete digitale Protokolle
  - 3.4 LTE
  - 3.5 5G
4. Telekom-Architektur
  - 4.1 Gesamtarchitektur
  - 4.2 Kern-Architektur
  - 4.3 Software-definierte Vernetzung
  - 4.4 5G-Campus-Netzwerke
  - 4.5 Sicherheit der Anwendungsschicht
5. Sicherheit von Handapparaten und Geräten
  - 5.1 Anforderungen
  - 5.2 Typischer Hardware-Entwurf
  - 5.3 IoT-Geräte
6. Bedrohungen
  - 6.1 Allgemeine Angriffsvektoren gegen (mobile) Geräte
  - 6.2 Allgemeine Angriffsvektoren gegen das Kernnetzwerk
  - 6.3 Mögliche Angriffe auf 5G-Campus-Netzwerke
7. Andere drahtlose Anwendungen
  - 7.1 Drahtlose Protokolle für Luftfahrt und Nautik
  - 7.2 Proprietäre Geräteprotokolle
  - 7.3 Großflächige Sensornetze (LoRa, Sigfox, ...)
  - 7.4 Digitale Sprach-/Datentechnologien (DECT/GAP, TETRA, ...)
  - 7.5 Satellitenkommunikation

- 8. Schutzmaßnahmen
  - 8.1 Mobile Technologie sicher integrieren
  - 8.2 Überwachung mobiler Geräte

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Bartock, M. / Cichonski, J. / Souppaya, M. (2020): 5G CYBERSECURITY: Preparing a Secure Evolution to 5G.
- Cichonski, J. / Franklin, J. M. / Bartock, M. (2017): Guide to LTE Security. NIST Special Publication 800-187.
- Mobile Threat Catalog, <https://pages.nist.gov/mobile-threat-catalogue/>
- Pavur, J. et al. (2020): A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In 2020 IEEE Symposium on Security and Privacy (S&P). IEEE. May, 2020.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

# Softwarearchitektur mobiler Geräte

Kurscode: DLBCSEEMT02\_D

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Mobile Geräte haben Desktops und Laptops als häufigste Endbenutzergeräte verdrängt. Das Smartphone ist zu einem zentralen Geschäftsinstrument geworden und User verwenden sie täglich für die unterschiedlichsten Anwendungen. Darüber hinaus nutzt auch das Internet der Dinge (IoT) diese mobilen Plattformen. Doch allzu oft sind die mit diesen mobilen Geräten verbundenen Risiken und Chancen insbesondere für die Sicherheitsadministratoren undurchsichtig, da diese Geräte oft außerhalb des traditionellen Intranets betrieben werden. In diesem Kurs untersuchen wir, wie die dominierenden Akteure, Android und Apple iOS, mit der Sicherheit in ihrem Softwarestack und ihrem Ökosystem umgehen. Wir betrachten auch das übersehene Problem der IoT-Sicherheit und schließen mit organisatorischen Lösungen ab.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Hardware- und Software-Stacks gängiger Mobiltelefone zu verstehen.
- die Sicherheitskontrollen in diesen Stacks verstehen.
- zu erkennen, welche Schutzmaßnahmen und Risiken mit den Ökosystemen der Geräte verbunden sind.
- zu erkennen, welche Angriffe in der Vergangenheit erfolgreich waren.
- die Verwaltung mobiler Endgeräte zum Schutz eines Unternehmens zu nutzen.

## Kursinhalt

1. Mobil-Technologie-Stacks
  - 1.1 Hardware
  - 1.2 Firmware
  - 1.3 Betriebssystem
  - 1.4 Bewerbungen
  - 1.5 Ökosystem

2. Hardware
  - 2.1 RF-Module
  - 2.2 PDA-Modul
  - 2.3 Trusted Execution Environment
  - 2.4 Biometrische Geräte
  - 2.5 Standorttechnik
3. Android-Betriebssystem
  - 3.1 Hardware
  - 3.2 Bootloader
  - 3.3 Kernel- und Hardware-Abstraktionsschicht
  - 3.4 Sandboxing und Virtualisierung
  - 3.5 Code-Unterzeichnung
4. Apple iOS-Betriebssystem
  - 4.1 Hardware
  - 4.2 Bootloader
  - 4.3 Kernel und Frameworks
  - 4.4 Sandboxing und Virtualisierung
  - 4.5 Code-Unterzeichnung
5. Mobile Geräte
  - 5.1 Das Internet der Dinge
  - 5.2 Linux
  - 5.3 RTOS
  - 5.4 Android auf Geräten
  - 5.5 Andere gebräuchliche eingebettete Betriebssysteme
6. Software-Ökosysteme und Sicherheit
  - 6.1 Google Play
  - 6.2 Apple Store
  - 6.3 Sicherheitsanbieter
  - 6.4 Die Rolle der Cloud
7. Bedrohungen von Mobiltelefonen
  - 7.1 Historische Beispiele für Angriffe auf Mobiltelefone
  - 7.2 Taxonomie der Bedrohungen von Mobiltelefonen
  - 7.3 Jailbreaking

- 8. Verwaltung mobiler Geräte
  - 8.1 Die Bedrohungen der BYOD
  - 8.2 Einzigartige Bedrohungen für mobile Geräte
  - 8.3 Verwaltung von Patches und Richtlinien

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Gupta, A. (2014): Learning Pentesting for Android Devices
- Mobile Threat Catalog, <https://pages.nist.gov/mobile-threat-catalogue/>
- N.A. (2020): Android Enterprise Security White Paper.
- N.A. (2019): iOS Security iOS 12.3. [https://www.apple.com/lae/business/docs/site/iOS\\_Security\\_Guide.pdf](https://www.apple.com/lae/business/docs/site/iOS_Security_Guide.pdf)
- Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBCSEEMT02\_D



# Supply Chain Management

Modulcode: BWSC

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> <ul style="list-style-type: none"> <li>▪ keine</li> <li>▪ keine</li> </ul>	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	---	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Tobias Specker (Supply-Chain-Management I) / Prof. Dr. Tobias Specker (Supply Chain Management II)

## Kurse im Modul

- Supply-Chain-Management I (BWSC01)
- Supply Chain Management II (BWSC02)

## Art der Prüfung(en)

<b>Modulprüfung</b>	<b>Teilmodulprüfung</b> <u>Supply-Chain-Management I</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten</li> <li>• Studienformat "myStudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90Min./- Minuten</li> <li>• Studienformat "Kombistudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit</li> </ul> <u>Supply Chain Management II</u> <ul style="list-style-type: none"> <li>• Studienformat "myStudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit,</li> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Hausarbeit</li> <li>• Studienformat "Fernstudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten</li> </ul>
<b>Anteil der Modulnote an der Gesamtnote</b> s. Curriculum	

<p><b>Lehrinhalt des Moduls</b></p> <p><b>Supply-Chain-Management I</b></p> <ul style="list-style-type: none"> <li>▪ Historische und terminologische Aspekte zum SCM-Konzept</li> <li>▪ Entstehungsmotive von unternehmensübergreifenden Wertschöpfungsnetzwerken</li> <li>▪ Gestaltungsprinzipien und Effekte von Wertschöpfungsnetzwerken</li> <li>▪ Logistische Kernprozesse und SCM</li> <li>▪ Informationstechnische Aspekte des SCM-Konzeptes</li> <li>▪ Koordination und Kollaboration der Netzwerkpartner</li> <li>▪ Branchenspezifische Lösungen des SCM</li> </ul> <p><b>Supply Chain Management II</b></p> <ul style="list-style-type: none"> <li>▪ Strategische Aspekte des SCMs</li> <li>▪ SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Planung</li> <li>▪ SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Beschaffung</li> <li>▪ SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Produktion</li> <li>▪ SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Distribution</li> </ul>
---

**Qualifikationsziele des Moduls**

**Supply-Chain-Management I**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Bedeutung unternehmensübergreifender Wertschöpfungsprozesse zu erklären.
- gängige Konzepte zur Modellierung unternehmensübergreifender Wertschöpfungsprozesse zu erklären.
- die dynamischen Effekte in Supply Chains zu erläutern und deren Ursache bzw. Wirkungseffekte zu systematisieren.
- wichtige theoretische Konzepte zur Beschreibung der Merkmale und Herausforderungen unternehmensübergreifender Wertschöpfungsprozesse zu skizzieren.
- die im Kontext des Supply Chain Managements gängigen Zugänge und Problemkategorien zu erklären.
- wichtige Referenz- und/oder Managementmodelle zur Konkretisierung von Supply Chain Systemen zu benennen.
- wichtige Rollen und Aufgaben im SCM-Netzwerk zu erläutern.
- das Koordinationsproblem des SCM die diesbezüglich gängigen Lösungsansätze zu beschreiben.

**Supply Chain Management II**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die strategische Relevanz unternehmensgreifender Wertschöpfungsprozesse in systematischer Weise zu erklären.
- die wichtigsten Aufgaben und Problem im SCM-Kernprozess Planung zu benennen.
- die Elemente und Zusammenhänge im CPFR-Modell in differenzierter Weise zu systematisieren.
- Merkmale und Besonderheiten der sog. Kontraktlogistik zu erläutern.
- die wichtigsten Aufgaben und Probleme im SCM-Kernprozess Beschaffung zu erklären.
- zentrale Elemente und Merkmale einer Beschaffungsstrategie zu erläutern.
- wichtigsten Aufgaben und Probleme im SCM-Kernprozess Produktion zu benennen.
- zentrale Elemente und Merkmale einer modernen Produktionsstrategie zu erläutern.
- die wichtigsten Aufgaben und Probleme im SCM-Kernprozess Distribution zu erklären.
- zentrale Elemente und Merkmale des sog. ECR-Konzeptes zu erläutern.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Transport & Logistik auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich Transport & Logistik

# Supply-Chain-Management I

Kurscode: BWSC01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

SCM erweist sich aus theoretischer wie praktischer Sicht als ein überaus facettenreiches Konstrukt. Ein problemadäquates Verständnis der Problemdimensionen und Wirkungsweisen (globaler) unternehmensübergreifender Wertschöpfungsnetzwerke bedingt einen mehrdimensionalen Zugang. Dessen Ausgangspunkt bildet die Beschäftigung mit logistischen Prozessen. Das darin nach modernen Maßstäben angestrebte Denken in Prozessen, Strömen und Netzwerken bildet eine wichtige Basis des SCM. Auf der Grundlage eines solchen Zugangs sollen die Studierenden in grundsätzlicher Weise mit dem SCM-Konzept vertraut gemacht werden. Unter dem Gesichtspunkt einer ganzheitlichen Betrachtung erweist es sich ferner als sinnvoll, neben den logistischen Herausforderungen dieses Konzeptes eine Reihe weiterer typischer Problemfelder zu beleuchten. Dies betrifft zum einen die informationstechnischen Aspekte des SCM (bspw. also APS-Systeme), zum anderen Fragen der Kollaboration und Koordination der Netzwerkpartner. Vervollständigt wird dieser Abriss schließlich mit der Betrachtung ausgewählter branchenspezifischer SCM-Lösungen (bspw. also ECR oder VMI).

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Bedeutung unternehmensübergreifender Wertschöpfungsprozesse zu erklären.
- gängige Konzepte zur Modellierung unternehmensübergreifender Wertschöpfungsprozesse zu erklären.
- die dynamischen Effekte in Supply Chains zu erläutern und deren Ursache bzw. Wirkungseffekte zu systematisieren.
- wichtige theoretische Konzepte zur Beschreibung der Merkmale und Herausforderungen unternehmensübergreifender Wertschöpfungsprozesse zu skizzieren.
- die im Kontext des Supply Chain Managements gängigen Zugänge und Problemkategorien zu erklären.
- wichtige Referenz- und/oder Managementmodelle zur Konkretisierung von Supply Chain Systemen zu benennen.
- wichtige Rollen und Aufgaben im SCM-Netzwerk zu erläutern.
- das Koordinationsproblem des SCM die diesbezüglich gängigen Lösungsansätze zu beschreiben.

**Kursinhalt**

1. Grundsätzliches zum Supply Chain-Konzept
  - 1.1 Terminologische und konzeptionelle Grundlagen
  - 1.2 Supply Chain-Typologie nach Otto
  - 1.3 Supply Chain-Typologie nach Bechtel/Jayaram
  - 1.4 Dynamische Aspekte von Supply Chains
2. Ausgewählte theoretische Konzepte zum Supply Chain-Konzept
  - 2.1 Neue Institutionenökonomik
  - 2.2 Spieltheorie
  - 2.3 Netzwerksansatz
  - 2.4 Sonstige theoretische Zugänge
3. Supply Chain Management
  - 3.1 Grundsätzliches zu Zielen und Spannweite des SCM
  - 3.2 Populäre Problemfelder des SCM
  - 3.3 Supply Chain Management als Evolutionsstufe der Logistik
  - 3.4 Supply Chain Management als Kooperationsmanagement
4. SCM-Modell
  - 4.1 Grundsätzliches zum Begriff SCM-Modelle
  - 4.2 SCOR-Modell
  - 4.3 SCM-Aufgabenmodell
5. SCM als Koordinationsproblem
  - 5.1 Grundsätzliches zum Koordinationsbegriff
  - 5.2 Koordinationskonzepte, -kontext und -perspektiven des SCM
  - 5.3 Koordinationsinstrumente

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Arndt, H. (2018): Supply Chain Management. Optimierung logistischer Prozesse. 7. Auflage, Gabler, Wiesbaden.
- Beckmann, H. (2012): Prozessorientiertes Supply Chain Engineering. Strategien, Konzepte und Methoden zur modellbasierten Gestaltung. Gabler-Verlag | Springer Fachmedien, Wiesbaden.
- Heiserich, O.E./Helbig, K./Ullmann, W. (2011): Logistik. Eine praxisorientierte Einführung. 4. Auflage, Gabler-Verlag | Springer Fachmedien, Wiesbaden 2011.
- Hungenberg, H. (2014): Strategisches Management in Unternehmen. Ziele-Prozesse-Verfahren. 8. Auflage, Wiesbaden.
- Pfohl, H. C. (2010): Logistiksysteme. Betriebswirtschaftliche Grundlagen. 8 Auflage, Springer, Berlin.
- Schulte, C. (2013): Logistik. Wege zur Optimierung der Supply Chain. 6. Auflage, Vahlen, München.
- Werner, H. (2013): Supply Chain Management. Grundlagen, Strategien, Instrumente und Controlling. 5. Auflage, Gabler, Wiesbaden.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b> 100 h	<b>Präsenzstudium</b> 0 h	<b>Tutorium</b> 25 h	<b>Selbstüberprüfung</b> 25 h	<b>Praxisanteil</b> 0 h	<b>Gesamt</b> 150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90Min./- Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b> 100 h	<b>Präsenzstudium</b> 0 h	<b>Tutorium</b> 25 h	<b>Selbstüberprüfung</b> 25 h	<b>Praxisanteil</b> 0 h	<b>Gesamt</b> 150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien



**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Schriftliche Ausarbeitung: Hausarbeit

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b> 100 h	<b>Präsenzstudium</b> 0 h	<b>Tutorium</b> 25 h	<b>Selbstüberprüfung</b> 25 h	<b>Praxisanteil</b> 0 h	<b>Gesamt</b> 150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien

# Supply Chain Management II

Kurscode: BWSC02

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Aus der Perspektive der strategischen Managementforschung und Praxis stehen die unter dem Begriff SCM gefassten Aktivitäten in enger Verbindung mit dem Bemühen zum Aufbau und/oder dem Erhalt erosionsstabiler betrieblicher Wettbewerbsvorteile. Eine grundsätzliche Erörterung dieses Zusammenhangs bildet den Ausgangspunkt dieses Kurses. Auf dieser Grundlage erfolgt danach im Rückgriff auf das sog. SCOR-Modell eine differenzierte Analyse von strategierelevanten Aktivitäten und Instrumenten im Bereich der Prozesskategorien Plan, Source, Make, Deliver und Return. Besondere Aufmerksamkeit wird dabei den praxisrelevanten Bereichen des SCMs gewidmet, bspw. also dem sog. Order-Promising (Plan), dem sog. Supplier-Relation-Management (Source), dem sog. Postponement (Make) oder dem sog. ECR-Konzept (Deliver).

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die strategische Relevanz unternehmensgreifender Wertschöpfungsprozesse in systematischer Weise zu erklären.
- die wichtigsten Aufgaben und Problem im SCM-Kernprozess Planung zu benennen.
- die Elemente und Zusammenhänge im CPFR-Modell in differenzierter Weise zu systematisieren.
- Merkmale und Besonderheiten der sog. Kontraktlogistik zu erläutern.
- die wichtigsten Aufgaben und Probleme im SCM-Kernprozess Beschaffung zu erklären.
- zentrale Elemente und Merkmale einer Beschaffungsstrategie zu erläutern.
- wichtigsten Aufgaben und Probleme im SCM-Kernprozess Produktion zu benennen.
- zentrale Elemente und Merkmale einer modernen Produktionsstrategie zu erläutern.
- die wichtigsten Aufgaben und Probleme im SCM-Kernprozess Distribution zu erklären.
- zentrale Elemente und Merkmale des sog. ECR-Konzeptes zu erläutern.

## Kursinhalt

1. Strategische Aspekte des SCM
  - 1.1 Strategisches Denken und Handeln: Grundsätzliches
  - 1.2 Wettbewerbsschwerpunkt und SCM
  - 1.3 Wettbewerbsort und SCM
  - 1.4 Wettbewerbsregeln und SCM

2. SCM-Praxis: Kernprozess Planung
  - 2.1 Allgemeine Vorüberlegungen
  - 2.2 Collaborative Planning, Forecasting and Replenishment
  - 2.3 Order Promising
  - 2.4 Kanban
  - 2.5 Integration von X-PL-Logistikdienstleistern
3. SCM-Praxis: Kernprozess Beschaffung
  - 3.1 Allgemeine Vorüberlegungen
  - 3.2 Produktionssynchrone Beschaffung
  - 3.3 Sourcing-Konzepte
  - 3.4 Supplier Relations Management
4. SCM-Praxis: Kernprozess Produktion
  - 4.1 Ausgewählte Aspekte zum Problemhintergrund
  - 4.2 Collaborative Engineering
  - 4.3 Postponement-Strategien
  - 4.4 Value Added Partnership
5. SCM-Praxis: Kernprozess Distribution
  - 5.1 Grundsätzliches zum Distributionsproblem
  - 5.2 Efficient Consumer Response (ECR)
  - 5.3 Konsignationslager

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Arndt, H. (2018): Supply Chain Management. Optimierung logistischer Prozesse. 7. Auflage, Gabler, Wiesbaden.
- Beckmann, H. (2012): Prozessorientiertes Supply Chain Engineering. Strategien, Konzepte und Methoden zur modellbasierten Gestaltung. Gabler-Verlag | Springer Fachmedien, Wiesbaden.
- Heiserich, O.E./Helbig, K./Ullmann, W. (2011): Logistik. Eine praxisorientierte Einführung. 4. Auflage, Gabler-Verlag | Springer Fachmedien, Wiesbaden 2011.
- Hungenberg, H. (2014): Strategisches Management in Unternehmen. Ziele-Prozesse-Verfahren. 8. Auflage, Wiesbaden.
- Pfohl, H. C. (2010): Logistiksysteme. Betriebswirtschaftliche Grundlagen. 8 Auflage, Springer, Berlin.
- Schulte, C. (2013): Logistik. Wege zur Optimierung der Supply Chain. 6. Auflage, Vahlen, München.
- Werner, H. (2013): Supply Chain Management. Grundlagen, Strategien, Instrumente und Controlling. 5. Auflage, Gabler, Wiesbaden.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Min./- Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b> 100 h	<b>Präsenzstudium</b> 0 h	<b>Tutorium</b> 25 h	<b>Selbstüberprüfung</b> 25 h	<b>Praxisanteil</b> 0 h	<b>Gesamt</b> 150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Hausarbeit

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
110 h	0 h	20 h	20 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b> 100 h	<b>Präsenzstudium</b> 0 h	<b>Tutorium</b> 25 h	<b>Selbstüberprüfung</b> 25 h	<b>Praxisanteil</b> 0 h	<b>Gesamt</b> 150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

BWSC02



# Smart Factory

Modulcode: DLBINGSF

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	--	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Christian Magnus (Smart Factory I ) / Prof. Dr. Christian Magnus (Smart Factory II)

## Kurse im Modul

- Smart Factory I (DLBINGSF01)
- Smart Factory II (DLBINGSF02)

## Art der Prüfung(en)

### Modulprüfung

### Teilmodulprüfung

#### Smart Factory I

- Studienformat "Kombistudium": *Prüfungsart*
- Studienformat "Fernstudium": Klausur,  
90 Minuten
- Studienformat "myStudium": *Prüfungsart*

#### Smart Factory II

- Studienformat "myStudium": *Prüfungsart*
- Studienformat "Fernstudium": Schriftliche  
Ausarbeitung: Projektbericht
- Studienformat "Kombistudium": *Prüfungsart*

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****Smart Factory I**

- Motivation und Begriffsabgrenzung
- Entwicklung der Automatisierung
- Technologische Grundlagen und Standards
- Grundkonzepte einer Smart Factory
- Referenzarchitekturen
- Smart Factory Engineering
- Sicherheit

**Smart Factory II**

Die Studierenden bearbeiten eine selbstgewählte Aufgabenstellung mithilfe einer Prototyping-Umgebung, die zum Gegenstand der Aufgabenstellung passt. Sie dokumentieren ihr Ergebnis mit einem Projektbericht.

**Qualifikationsziele des Moduls****Smart Factory I**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Begriff Smart Factory zu erläutern und in den Kontext Industrie 4.0 einzuordnen.
- die Entwicklung der Automatisierung bis zur vollautonomen, dezentral organisierten Produktionsanlage zu skizzieren.
- die grundlegenden Technologien und Standards zu benennen, die für den Entwurf und Betrieb einer Smart Factory eingesetzt werden.
- die wesentlichen Konzepte einer Smart Factory darzustellen.
- die einzelnen Elemente einer Smart Factory anhand verschiedener Referenzarchitekturen zu identifizieren und voneinander abzugrenzen.
- die besonderen Engineering-Herausforderungen im Smart Energy-Kontext herauszustellen.
- die speziellen sicherheitstechnischen Risiken digitalisierter und vernetzter Produktionsanlagen zu erläutern und ihnen jeweils konkrete Handlungsempfehlungen zuzuordnen.

**Smart Factory II**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Technologien und Standards im Kontext Smart Factory zu durchdringen.
- Technologien im Kontext Smart Factory an einem einfachen Praxisbeispiel anzuwenden.
- zu einer ausgewählten Aufgabenstellung einen Hardware- oder Software-Prototypen zu entwerfen.
- Entwurfs- und Entwicklungstätigkeiten in Form eines Projektberichts zu dokumentieren.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Smart Factory I

Kurscode: DLBINGSF01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

In diesem Kurs sollen die Studierenden einen vertieften Einblick in die Vernetzung und Digitalisierung von Produktionsanlagen im Sinne einer Smart Factory erhalten. Hierzu werden sie mit den grundlegenden Zielen einer Smart Factory im Kontext des Forschungskomplexes Industrie 4.0 vertraut gemacht. Nach einer kurzen Einführung in die Geschichte der Automatisierung werden den Studierenden die technischen Grundlagen und Standards vermittelt, die für den Entwurf und den Betrieb einer Smart Factory erforderlich sind. Darauf aufbauend wird gezeigt, wie diese einzelnen Technologien eingesetzt werden, um die zentralen Konzepte einer Smart Factory zu realisieren. Um zu verstehen, aus welchen Bestandteilen eine Smart Factory besteht, werden verschiedene Referenzarchitekturen vor- und gegenübergestellt. Der Kurs schließt mit den besonderen Engineering-Herausforderungen einer autonom handelnden und dezentral organisierten Produktionsanlage. Dazu zählt vor allem der Aspekt der IT-Sicherheit, der durch die digitale Vernetzung der Produktionsanlagen und Produkte besonders relevant ist.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Begriff Smart Factory zu erläutern und in den Kontext Industrie 4.0 einzuordnen.
- die Entwicklung der Automatisierung bis zur vollautonomen, dezentral organisierten Produktionsanlage zu skizzieren.
- die grundlegenden Technologien und Standards zu benennen, die für den Entwurf und Betrieb einer Smart Factory eingesetzt werden.
- die wesentlichen Konzepte einer Smart Factory darzustellen.
- die einzelnen Elemente einer Smart Factory anhand verschiedener Referenzarchitekturen zu identifizieren und voneinander abzugrenzen.
- die besonderen Engineering-Herausforderungen im Smart Energy-Kontext herauszustellen.
- die speziellen sicherheitstechnischen Risiken digitalisierter und vernetzter Produktionsanlagen zu erläutern und ihnen jeweils konkrete Handlungsempfehlungen zuzuordnen.

**Kursinhalt**

1. Motivation und Begriffsabgrenzung
  - 1.1 Ziele von Smart Factory
  - 1.2 Internet of Things
  - 1.3 Cyber-physische Systeme
  - 1.4 Cyber-physische Produktionssysteme
  - 1.5 Smart Factory als Cyber-physisches (Produktions-)System
2. Entwicklung der Automatisierung
  - 2.1 Automatisierungspyramide
  - 2.2 Vernetzte, dezentrale Organisation der Produktion
  - 2.3 Zukünftige Herausforderungen
3. Technologische Grundlagen und Standards
  - 3.1 Identifizierung physikalischer Objekte
  - 3.2 Formale Beschreibungssprachen und Ontologien
  - 3.3 Digitales Objektgedächtnis
  - 3.4 Physikalische Situationserkennung
  - 3.5 (Teil-)autonomes Handeln und Kooperieren
  - 3.6 Mensch-Maschine-Interaktion
  - 3.7 Maschine-Maschine-Kommunikation
4. Grundkonzepte einer Smart Factory
  - 4.1 Auftragsgesteuerte Produktion
  - 4.2 Bündelung von Maschinen- und Produktionsdaten
  - 4.3 Unterstützung des Menschen in der Produktion
  - 4.4 Intelligente Produkte und Betriebsmittel
  - 4.5 Smart Services
5. Referenzarchitekturen
  - 5.1 Zweck und Eigenschaften von Referenzarchitekturen
  - 5.2 Überblick über Normungsinitiativen
  - 5.3 CyProS-Referenzarchitektur
  - 5.4 RAMI 4.0 (DIN SPEC 91345)

6. Smart Factory Engineering
  - 6.1 Klassifikation verschiedener Engineering-Werkzeuge
  - 6.2 Virtual Engineering
  - 6.3 User-Centered Design
  - 6.4 Requirements Engineering
  - 6.5 Modellierung
  - 6.6 Integration klassischer und smarterer Komponenten
7. Sicherheit
  - 7.1 Sicherheitsrisiken in einer Smart Factory
  - 7.2 Handlungsvorschläge des BMWi
  - 7.3 VDMA-Handlungsleitfaden

## Literatur

### Pflichtliteratur

#### Weiterführende Literatur

- Bangemann, T. et al. (2016): Integration of Classical Components into Industrial Cyber-Physical Systems. In: Proceedings of the IEEE, 104. Jg., Heft 5, S. 947–959. DOI: 10.1109/JPROC.2015.2510981.
- Bauernhansl, T./Hompe, M. ten/Vogel-Heuser, B. (Hrsg.) (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Springer, Berlin.
- Bundesministerium für Wirtschaft und Energie (Hrsg.) (2016): IT-Sicherheit für die Industrie 4.0. Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten. Berlin.
- Geisberger, E./Broy, M. (Hrsg.) (2012): agendaCPS. Integrierte Forschungsagenda Cyber-Physical Systems. Springer, Berlin/Heidelberg.
- Harrison, R./Vera, D./Ahmad, B. (2016): Engineering Methods and Tools for Cyber-Physical Automation Systems. In: Proceedings of the IEEE, 104. Jg., Heft 5, S. 973–985. DOI: 10.1109/JPROC.2015.2510665.
- Haupt, J. (2013): DOMEMan: Repräsentation, Verwaltung und Nutzung von digitalen Objektgedächtnissen. Akademische Verlagsgesellschaft AKA, Berlin.
- VDMA & Partner (2016): Leitfaden Industrie 4.0 Security. Handlungsempfehlungen für den Mittelstand. VDMA Verlag, Frankfurt a. M.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b>
------------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input checked="" type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien



**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b>
---------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

## Smart Factory II

Kurscode: DLBINGSF02

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

### Beschreibung des Kurses

In diesem Kurs wählen die Studierenden in Abstimmung mit dem Seminarleiter eine konkrete Aufgabenstellung aus dem bereitgestellten Themenkatalog aus. Sie bearbeiten die Aufgabe mithilfe einer Prototyping-Umgebung, die zum Gegenstand der Aufgabenstellung passt. Bei den Umgebungen kann es sich sowohl um Hardware (z. B. Prototyping-Boards) als auch um Software (z. B. technologiespezifische Entwicklungsumgebungen) handeln. Zur Bearbeitung der Aufgabe wenden die Studierenden die im Kurs Smart Factory I vermittelten Konzepte, Methoden und Werkzeuge an. Sie dokumentieren ihr Ergebnis mit einem Projektbericht.

### Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Technologien und Standards im Kontext Smart Factory zu durchdringen.
- Technologien im Kontext Smart Factory an einem einfachen Praxisbeispiel anzuwenden.
- zu einer ausgewählten Aufgabenstellung einen Hardware- oder Software-Prototypen zu entwerfen.
- Entwurfs- und Entwicklungstätigkeiten in Form eines Projektberichts zu dokumentieren.

### Kursinhalt

- Ein Katalog mit den jeweils aktuell bereitgestellten Aufgabenstellungen wird auf der Online-Plattform des Moduls bereitgestellt. Er bietet die inhaltliche Basis des Moduls und kann vom Seminarleiter ergänzt bzw. aktualisiert werden.

### Literatur

#### Pflichtliteratur

#### Weiterführende Literatur

- Themenspezifische Literaturlauswahl

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b>
---------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b>
------------------------------------	----------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input type="checkbox"/> Folien

DLBINGSF02

# Robotics und Automatisierung

Modulcode: DLBCSDWRA

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

Prof. Dr. Mario Boßlau (Fertigungsverfahren Industrie 4.0) / Prof. Dr. Torsten Bruns (Automatisierung und Robotics)

## Kurse im Modul

- Fertigungsverfahren Industrie 4.0 (DLBINGFVI01)
- Automatisierung und Robotics (DLBINGAUR01)

## Art der Prüfung(en)

### Modulprüfung

### Teilmodulprüfung

#### Fertigungsverfahren Industrie 4.0

- Studienformat "Fernstudium": Klausur, 90 Minuten
- Studienformat "Kombistudium": Klausur, 90 Minuten
- Studienformat "myStudium": Klausur, 90 Minuten

#### Automatisierung und Robotics

- Studienformat "Kombistudium": Klausur, 90 Minuten
- Studienformat "Fernstudium": Klausur, 90 Minuten

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

### **Lehrinhalt des Moduls**

#### **Fertigungsverfahren Industrie 4.0**

- Einführung in die Fertigungstechnik
- Fertigungshauptgruppen nach DIN 8580
- Additive Fertigungsverfahren
- Rapid Prototyping
- Rapid Tooling
- Direct/Rapid Manufacturing
- Cyber-physische Produktionsanlagen

#### **Automatisierung und Robotics**

- Grundlagen der Automatisierung
- Grundlagen der Messtechnik
- Sensoren
- Grundlagen der Regelungstechnik
- Grundlagen der Steuerungstechnik
- Einführung in die Robotik
- Kinematik eines Roboters



**Qualifikationsziele des Moduls****Fertigungsverfahren Industrie 4.0**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Begriffe und Zusammenhänge der Fertigungstechnik zu erklären.
- die aktuellen Veränderungen in der Fertigungstechnik durch Technologien wie der Additiven Fertigung und Megatrends wie Cyber Physical Systems darzustellen.
- verschiedene Fertigungsverfahren den Fertigungshauptgruppen nach DIN 8580 zuzuordnen.
- das grundlegende Prinzip additiver Fertigungsverfahren zu erklären.
- verschiedene additive Fertigungsverfahren voneinander abzugrenzen.
- die Begriffe Rapid Prototyping, Rapid Tooling und Direct Manufacturing zu erläutern und ihnen jeweils einzelne Verfahren und Anwendungsbeispiele zuzuordnen.
- die Elemente und Eigenschaften Cyber-physischer Produktionsanlagen zu erklären.

**Automatisierung und Robotics**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Aspekte der Automatisierung zu erläutern.
- die verschiedenen Größen und Einheiten in der Messtechnik zu benennen.
- verschiedene Messmethoden voneinander abzugrenzen.
- den grundlegenden Aufbau von Messeinrichtungen zu beschreiben.
- einen geeigneten Sensor anhand verschiedener Kriterien auszuwählen.
- die Elemente von Regelungssystemen zu benennen.
- das Verhalten von Regelsystemen im Zeit- und Frequenzbereich zu beschreiben.
- grundlegende Prinzipien der Steuerungstechnik zu beschreiben.
- zwischen verschiedenen Zahlensystemen umzurechnen und die Boolesche Algebra anzuwenden.
- den Aufbau von Schaltnetzen, -werken und Speichern zu beschreiben.
- wichtige Elemente von Steuerungssystemen wie Signalgeneratoren und Leistungsverstärker zu benennen.
- einfache speicherprogrammierbare Steuerungen zu entwerfen.
- den grundlegenden Aufbau von Industrierobotern zu beschreiben.
- verschiedene Bewegungen und Positionen von Gelenkarmrobotern zu berechnen.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Ingenieurwissenschaften und Informatik & Software-Entwicklung auf.

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik.

# Fertigungsverfahren Industrie 4.0

Kurscode: DLBINGFVI01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden, ausgehend von traditionellen, standardisierten Fertigungstechniken, einen Überblick über solche Verfahren zu bieten, die durch technologische Entwicklungen unter dem Oberbegriff Industrie 4.0 die Produktionsprozesse beeinflusst haben und noch beeinflussen. Dazu zählen insbesondere technologische Fortschritte bei den additiven Fertigungsverfahren, die Anwendungen wie das Rapid Prototyping, Rapid Tooling und das Direct Manufacturing ermöglichen. Abschließend behandelt der Kurs die Folgen der Digitalisierung und Vernetzung von Produktionsanlagen und deren Elemente im Sinne eines Cyber-physischen Systems.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Begriffe und Zusammenhänge der Fertigungstechnik zu erklären.
- die aktuellen Veränderungen in der Fertigungstechnik durch Technologien wie der Additiven Fertigung und Megatrends wie Cyber Physical Systems darzustellen.
- verschiedene Fertigungsverfahren den Fertigungshauptgruppen nach DIN 8580 zuzuordnen.
- das grundlegende Prinzip additiver Fertigungsverfahren zu erklären.
- verschiedene additive Fertigungsverfahren voneinander abzugrenzen.
- die Begriffe Rapid Prototyping, Rapid Tooling und Direct Manufacturing zu erläutern und ihnen jeweils einzelne Verfahren und Anwendungsbeispiele zuzuordnen.
- die Elemente und Eigenschaften Cyber-physischer Produktionsanlagen zu erklären.

## Kursinhalt

1. Einführung in die Fertigungstechnik
  - 1.1 Grundlegende Begriffe und Zusammenhänge in der Fertigungslehre
  - 1.2 Historische Entwicklung der Fertigung
  - 1.3 Die Diskussion über den Long Tail

2. Fertigungshauptgruppen nach DIN 8580
  - 2.1 Urformen
  - 2.2 Umformen
  - 2.3 Trennen (Zerteilen, Zerspanung, Abtragen)
  - 2.4 Fügen
  - 2.5 Beschichten
  - 2.6 Stoffeigenschaftsändern
3. Additive Fertigungsverfahren
  - 3.1 Grundprinzip und rechtliche Aspekte
  - 3.2 Stereolithographie (STL)
  - 3.3 Selektives Lasersintern und selektives Strahlschmelzen mit Laser- oder Elektronenstrahl
  - 3.4 Fused Deposition Modeling (FDM)
  - 3.5 Multi-Jet Modeling (MJM) und Poly-Jet-Verfahren (PJM)
  - 3.6 3D-Druckverfahren (3DP)
  - 3.7 Laminierverfahren
  - 3.8 Maskensintern
4. Rapid Prototyping
  - 4.1 Begriffsbestimmung
  - 4.2 Strategische und operative Aspekte
  - 4.3 Anwendungsgebiete und -beispiele
5. Rapid Tooling
  - 5.1 Begriffsbestimmung, strategische und operative Aspekte
  - 5.2 Indirekte und direkte Verfahren
6. Direct/Rapid Manufacturing
  - 6.1 Potentiale und Anforderungen an die Verfahren
  - 6.2 Umsetzung, Anwendungsgebiete und -beispiele
7. Cyber-physische Produktionsanlagen
  - 7.1 Herleitung der Begriffe Industrie 4.0 und Cyber-physische Systeme
  - 7.2 Megatrend Cyber Physical Systems (CPS)
  - 7.3 Definition Cyber-physische Produktionsanlage
  - 7.4 Auswirkungen auf Planung und Betrieb von Produktionsanlagen
  - 7.5 Dynamische Rekonfiguration und Migration von Produktionsanlagen

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Bauernhansl, T./ten Hompel, M./Vogel-Heuser, B. (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Springer Vieweg, Wiesbaden.
- Behmel, M. et al. (2019): Industrielle Fertigung: Fertigungsverfahren, Mess- und Prüftechnik. 8. Auflage, Verlag Europa-Lehrmittel, Haan-Gruiten.
- Botthoff, A./Hartmann, E. A. (2015) (Hrsg.): Zukunft der Arbeit in Industrie 4.0. Springer Vieweg, Wiesbaden.
- Brecher, C. (2015): Advances in Production Technology. Springer Cham, Heidelberg u. a.
- Fritz, A. H. (Hrsg.) (2018): Springer-Lehrbuch. Fertigungstechnik. 12. Auflage. Springer Vieweg, Wiesbaden.
- Gummersbach, A. et al. (2017): Produktionsmanagement. 6 Auflage, Handwerk und Technik, Hamburg.
- Huber, W. (2016): Industrie 4.0 in der Automobilproduktion. Springer Fachmedien, Wiesbaden.
- Schmid, D. (2013): Produktion – Technologie und Management. Verlag Europa-Lehrmittel Haan-Gruiten.
- Westkämper, E./Warnecke, H.-J. (2010): Einführung in die Fertigungstechnik. 8. Auflage, Springer Fachmedien, Wiesbaden.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Vorlesung
---------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input type="checkbox"/> Folien

# Automatisierung und Robotics

Kurscode: DLBINGAUR01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen Einblick in die Mess-, Regel- und Steuerungstechnik zu bieten sowie die Grundlagen der Robotik zu vermitteln. Hierzu wird den Studierenden dargelegt, mit welchen Methoden bestimmte Messgrößen ermittelt werden können und wie mit Messfehlern umgegangen wird. Auf diesen Grundlagen aufbauend werden verschiedene Sensoren vorgestellt und die Studierenden dazu befähigt, passende Sensoren anhand vorgegebener Kriterien auszuwählen. Der Kurs führt die Studierenden darüber hinaus in die Grundlagen der Regelungstechnik ein. Dabei werden den Studierenden die verschiedenen Möglichkeiten zur Beschreibung der Struktur und des Verhaltens von Regelsystemen veranschaulicht. Neben der Regelungstechnik werden auch die Grundlagen der Steuerungstechnik vermittelt. Die Studierenden erhalten eine kurze Einführung in binäre Zahlensysteme und die Boolesche Algebra und setzen sich darüber hinaus mit verschiedenen basalen Schaltungs- und Steuerungselementen auseinander. Zuletzt erhalten die Studierenden einen Einblick in die Robotik mit einem Schwerpunkt auf Industrieroboter. In diesem Zusammenhang erlernen die Studierenden die Beschreibung und Berechnung von Positionen und Bewegungen einzelner Glieder eines Roboterarms.



**Kursziele**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Aspekte der Automatisierung zu erläutern.
- die verschiedenen Größen und Einheiten in der Messtechnik zu benennen.
- verschiedene Messmethoden voneinander abzugrenzen.
- den grundlegenden Aufbau von Messeinrichtungen zu beschreiben.
- einen geeigneten Sensor anhand verschiedener Kriterien auszuwählen.
- die Elemente von Regelungssystemen zu benennen.
- das Verhalten von Regelsystemen im Zeit- und Frequenzbereich zu beschreiben.
- grundlegende Prinzipien der Steuerungstechnik zu beschreiben.
- zwischen verschiedenen Zahlensystemen umzurechnen und die Boolesche Algebra anzuwenden.
- den Aufbau von Schaltnetzen, -werken und Speichern zu beschreiben.
- wichtige Elemente von Steuerungssystemen wie Signalgeneratoren und Leistungsverstärker zu benennen.
- einfache speicherprogrammierbare Steuerungen zu entwerfen.
- den grundlegenden Aufbau von Industrierobotern zu beschreiben.
- verschiedene Bewegungen und Positionen von Gelenkarmrobotern zu berechnen.

**Kursinhalt**

1. Grundlagen der Automatisierung
  - 1.1 Grundlegende Begriffe
  - 1.2 Wirtschaftliche Aspekte
  - 1.3 Automatisierungspyramide
  - 1.4 Mess-, Steuer- und Regelsysteme
2. Grundlagen der Messtechnik
  - 2.1 Messgrößen und Einheiten
  - 2.2 Formen von Messsignalen
  - 2.3 Messmethoden
  - 2.4 Messeinrichtungen
  - 2.5 Bewertung von Messungen und Messfehler

3. Sensoren
  - 3.1 Funktion und Elemente von Sensoren
  - 3.2 Kriterien zur Auswahl von Sensoren
  - 3.3 Näherungsschalter
  - 3.4 Fotoelektrische Sensoren
  - 3.5 Ultraschallsensoren
  - 3.6 Drehgeber
  - 3.7 Kraft-, Drehmoment- und Druckmesser
  - 3.8 Temperatursensoren
  - 3.9 Bildverarbeitende Sensoren
4. Grundlagen der Regelungstechnik
  - 4.1 Elemente von Regelungssystemen
  - 4.2 Strukturbeschreibung
  - 4.3 Statische Verhaltensbeschreibung
  - 4.4 Verhaltensbeschreibung im Zeitbereich
  - 4.5 Verhaltensbeschreibung im Frequenzbereich
  - 4.6 Praxisbeispiele
5. Grundlagen der Steuerungstechnik
  - 5.1 Grundprinzip und Elemente von Steuerungssystemen
  - 5.2 Zahlendarstellungen
  - 5.3 Boolesche Algebra
  - 5.4 Schaltnetze, -werke und Speicher
  - 5.5 Signalgeneratoren und Leistungsverstärker
  - 5.6 Speicherprogrammierbare Steuerungen
  - 5.7 Verbindungsprogrammierte Steuerungen
6. Einführung in die Robotik
  - 6.1 Begriffe und Einordnung
  - 6.2 Grundlegende Elemente
  - 6.3 Klassifikation von Robotern
7. Kinematik eines Roboters
  - 7.1 Koordinatensysteme und Bezugspunkte
  - 7.2 Rotationen
  - 7.3 Vorwärts- und Rückwärtstransformationen

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Heinrich, B./Linke, P./Glöckler, M. (2015): Grundlagen Automatisierung. Springer, Wiesbaden.
- Hesse, S./Malisa, V. (Hrsg.) (2016): Taschenbuch Robotik – Montage – Handhabung. 2. Auflage, Carl Hanser Verlag, München.
- Jazar, R. N. (2010): Theory of Applied Robotics. 2. Auflage, Springer US, Boston (MA).
- Karaali, C. (2013): Grundlagen der Steuerungstechnik. Springer, Wiesbaden.
- Parthier, R. (2011): Messtechnik. Grundlagen und Anwendungen der elektrischen Messtechnik für alle technischen Fachrichtungen und Wirtschaftsingenieure. 6. Auflage, Vieweg & Teubner, Wiesbaden.
- Tietze, U./Schenk, C./Gamm, E. (2016): Halbleiter-Schaltungstechnik. 15. Auflage, Springer, Berlin.
- Zacher, S./Reuter, M. (2014): Regelungstechnik für Ingenieure. Springer, Wiesbaden.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Vorlesung
------------------------------------	-----------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
90 h	0 h	30 h	30 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input checked="" type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input type="checkbox"/> Prüfungsleitfaden
<input checked="" type="checkbox"/> Shortcast	<input checked="" type="checkbox"/> Live Tutorium/Course Feed
<input checked="" type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input checked="" type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLBINGAUR01

# Mobile Software Engineering

Modulcode: IWMB

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	--	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

## Modulverantwortliche(r)

Prof. Dr. Marian Benner-Wickner (Mobile Software Engineering am Beispiel der Android-Plattform) / Prof. Dr. Marian Benner-Wickner (Projekt Mobile Software Engineering)

## Kurse im Modul

- Mobile Software Engineering am Beispiel der Android-Plattform (IWMB01)
- Projekt Mobile Software Engineering (IWMB02)

## Art der Prüfung(en)

### Modulprüfung

### Teilmodulprüfung

Mobile Software Engineering am Beispiel der Android-Plattform

- Studienformat "Fernstudium": Klausur oder Schriftliche Ausarbeitung: Fallstudie, 90 Minuten

Projekt Mobile Software Engineering

- Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht
- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

## Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****Mobile Software Engineering am Beispiel der Android-Plattform**

- Grundlagen der mobilen Software-Entwicklung
- Android-Systemarchitektur
- Entwicklungsumgebung
- Kernkomponenten einer Android-App
- Interaktion zwischen Anwendungskomponenten
- Fortgeschrittene Techniken

**Projekt Mobile Software Engineering**

Konzeption, Umsetzung und Dokumentation von kleinen, mobilen Anwendungen auf Basis einer konkreten Aufgabenstellung.

**Qualifikationsziele des Moduls****Mobile Software Engineering am Beispiel der Android-Plattform**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Unterschiede und Besonderheiten der SW-Entwicklung für mobile Systeme zu erkennen und diese zu erläutern.
- verschiedene Aktivitäten, Rollen und Risiken bei Erstellung, Betrieb und Wartung von mobilen Software-Systemen zu unterscheiden.
- Architektur und technische Eigenschaften der Android Plattform zu erläutern und zu unterscheiden.
- selbstständig mobile Software-Systeme zur Lösung von konkreten Problemen für die Plattform „Android“ zu erstellen.

**Projekt Mobile Software Engineering**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine kleine mobile Anwendung zu konzipieren und prototypisch zu erstellen, um eine gezielte Aufgabe zu lösen.
- typische Probleme und Herausforderungen in der praktischen Umsetzung kleiner mobiler Anwendungen zu erkennen.
- die Konzeption und die Umsetzung von kleinen, eigenständig konzipiert und umgesetzten mobilen Anwendungen zu dokumentieren.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik



# Mobile Software Engineering am Beispiel der Android-Plattform

Kurscode: IWMB01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Am Beispiel der mobilen Plattform „Android“ wird vermittelt, wie sich die Programmierung von mobilen Anwendungen (Apps) von der Entwicklung von Browser-basierten Informationssystemen unterscheidet, welche Technologien und Programmierkonzepte typischerweise dabei zum Einsatz kommen und welche typischen Herausforderungen es bei der App-Entwicklung für industrielle Anwendungen gibt.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Unterschiede und Besonderheiten der SW-Entwicklung für mobile Systeme zu erkennen und diese zu erläutern.
- verschiedene Aktivitäten, Rollen und Risiken bei Erstellung, Betrieb und Wartung von mobilen Software-Systemen zu unterscheiden.
- Architektur und technische Eigenschaften der Android Plattform zu erläutern und zu unterscheiden.
- selbstständig mobile Software-Systeme zur Lösung von konkreten Problemen für die Plattform „Android“ zu erstellen.

## Kursinhalt

1. Grundlagen der mobilen Software-Entwicklung
  - 1.1 Besonderheiten von mobilen Endgeräten
  - 1.2 Besonderheiten der mobilen Software-Entwicklung
  - 1.3 Einteilung von mobilen Endgeräten
  - 1.4 Die Android-Plattform
2. Android-Systemarchitektur
  - 2.1 Das Android-System
  - 2.2 Sicherheit
  - 2.3 Kommunikation mit Netzwerken

3. Entwicklungsumgebung
  - 3.1 Android Studio
  - 3.2 Erste App und Emulator-Test
  - 3.3 Anwendungsdeployment
4. Kernkomponenten einer Android-App
  - 4.1 Überblick über die Komponenten einer Android-App
  - 4.2 Activities, Layouts und Views
  - 4.3 Ressourcen
  - 4.4 Zusammenfassung in einer App
  - 4.5 Grafische Gestaltung
5. Interaktion zwischen Anwendungskomponenten
  - 5.1 Intents
  - 5.2 Services
  - 5.3 Broadcast Receive
6. Fortgeschrittene Techniken
  - 6.1 Threading
  - 6.2 Anwendungsspeicher

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Google Inc. (2022a): Android Developer Guides.
- Richter, E. (2021): Android-Apps programmieren: Professionelle App-Entwicklung mit Android Studio 4. 3. Auflage, mitp, Frechen.
- Vollmer, G. (2017): Mobile App Engineering: eine systematische Einführung - von den Requirements zum Go Live. 1. Auflage, dpunkt, Heidelberg.

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Online-Vorlesung
-----------------------------------	------------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Ja
<b>Prüfungsleistung</b>	Klausur oder Schriftliche Ausarbeitung: Fallstudie, 90 Minuten

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b> 100 h	<b>Präsenzstudium</b> 0 h	<b>Tutorium</b> 25 h	<b>Selbstüberprüfung</b> 25 h	<b>Praxisanteil</b> 0 h	<b>Gesamt</b> 150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input type="checkbox"/> Reader <input checked="" type="checkbox"/> Folien

# Projekt Mobile Software Engineering

Kurscode: IWMB02

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Die Studierenden erstellen selbständig eine mobile Anwendung und dokumentieren deren Konzeption und Umsetzung.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine kleine mobile Anwendung zu konzipieren und prototypisch zu erstellen, um eine gezielte Aufgabe zu lösen.
- typische Probleme und Herausforderungen in der praktischen Umsetzung kleiner mobiler Anwendungen zu erkennen.
- die Konzeption und die Umsetzung von kleinen, eigenständig konzipiert und umgesetzten mobilen Anwendungen zu dokumentieren.

## Kursinhalt

- Konzeption, Umsetzung und Dokumentation von kleinen, mobilen Anwendungen auf Basis einer konkreten Aufgabenstellung.  
Mögliche Themen sind zum Beispiel:
- Eine Radio-App, um den Austausch zwischen Hörer und Sender allgemein, aber vor allem zwischen Hörern und Radiomoderatoren zu verbessern.
- Eine App, mit der eine Gruppe von Brettspielfans ihren regelmäßigen abendlichen Spieltermin besser organisieren kann.
- Eine App, mit der die Betreuer von Abschlussarbeiten an der IUBH ihre Betreuungsprozesse verbessern können.

**Literatur****Pflichtliteratur****Weiterführende Literatur**

- Becker, A./Pant, M. (2015): Android 5. Programmieren für Smartphones und Tablets. 4. Auflage, dpunkt, Heidelberg.
- Eason, J. (2014): Android Studio 1.0. (URL: <http://android-developers.blogspot.de/2014/12/android-studio-10.html> [letzter Zugriff: 12.06.2015]).
- Franke, F./Ippen, J. (2012): Apps mit HTML5 und CSS3. Rheinwerk Verlag, Bonn.
- Google Inc. (Hrsg.) (2015): Android Developer Guide. (URL: <http://developer.android.com/guide>)
- Google Inc. (Hrsg.) (2015a): App Components. (URL: <http://developer.android.com/guide/components/index.html> [letzter Zugriff: 12.06.2015]).
- Google Inc. (Hrsg.) (2015b): Installing the Android SDK. (URL: <http://developer.android.com/sdk/installing/index.html> [letzter Zugriff: 13.05.2015]).
- Google Inc. (Hrsg.) (2015c): Resources Overview. (URL: <http://developer.android.com/guide/topics/resources/overview.html> [letzter Zugriff: 12.06.2015]).
- Hipp, Wyrick & Company, Inc. (Hrsg.) (2015): SQLite Webseite. (URL: <http://sqlite.org/index.html> [letzter Zugriff: 12.06.2015]).
- Künneht, T. (2016): Android 7. Das Praxisbuch für Entwickler. 4. Auflage, Rheinwerk, Bonn.
- Ross, M. (2013): Apache Cordova. Eine praktische Einführung in die mobile Cross-Plattform-Entwicklung mit PhoneGap. dpunkt Verlag, Heidelberg.
- Post, U. (2014): Android Apps entwickeln. Eigene Spiele-Apps für Leser mit Programmierkenntnissen. 4. Auflage, Galileo Computing, Bonn.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Projekt
------------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

IWMB02



# Apple Mobile Solution Development

Modulcode: DLAMSD

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	Für die Teilnahme an diesem Kurs wird ein Mac-Computer (z.B. MacBook, iMac) mit einem aktuellen macOS-Betriebssystem benötigt. Zur App-Entwicklung wird die im Mac-App-Store zur Verfügung gestellte Entwicklungsumgebung Xcode eingesetzt.	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

## Modulverantwortliche(r)

Prof. Dr. Sandra Rebholz (Apple Mobile Solution Development I) / Prof. Dr. Sandra Rebholz (Apple Mobile Solution Development II)

## Kurse im Modul

- Apple Mobile Solution Development I (DLAMSD01)
- Apple Mobile Solution Development II (DLAMSD02)

## Art der Prüfung(en)

<b>Modulprüfung</b>	<b>Teilmodulprüfung</b> <u>Apple Mobile Solution Development I</u> <ul style="list-style-type: none"> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul> <u>Apple Mobile Solution Development II</u> <ul style="list-style-type: none"> <li>• Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht</li> <li>• Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht</li> </ul>
<b>Anteil der Modulnote an der Gesamtnote</b> s. Curriculum	

<p><b>Lehrinhalt des Moduls</b></p> <p><b>Apple Mobile Solution Development I</b></p> <p>In diesem Kurs erhalten die Studierenden eine fundierte Einführung in die mobile App-Entwicklung auf der iOS-Plattform von Apple. Im Rahmen des Kurses lernen die Studierenden sowohl die grundlegenden Konzepte der objektorientierten Programmierung mit Swift kennen, als auch geeignete Methoden und professionelle Werkzeuge zum App-Design und zur App-Entwicklung.</p> <p><b>Apple Mobile Solution Development II</b></p> <p>In diesem Kurs befassen sich die Studierenden mit fortgeschrittenen Konzepten der mobilen App-Entwicklung auf der iOS-Plattform von Apple. Die Studierenden durchlaufen dabei den gesamten App-Design- und Entwicklungsprozess und nutzen aktuelle Frameworks und Best-Practices zum Entwurf und zur Umsetzung eigener interaktiver iOS-Apps.</p>
--

**Qualifikationsziele des Moduls****Apple Mobile Solution Development I**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte und Sprachkonstrukte der Programmiersprache Swift im Kontext eines Programms zu erklären.
- für vorgegebene Aufgabenstellungen einen passenden Algorithmus zu entwickeln und diesen in Form eines Swift-Programmes umzusetzen.
- geeignete Methoden und Werkzeuge zur App-Entwicklung mit Swift einzusetzen.
- den grundlegenden Aufbau einer iOS-App und deren Komponenten zu erläutern.
- eine einfache interaktive iOS-App zu entwickeln.

**Apple Mobile Solution Development II**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- fortgeschrittene Programmier Techniken zur Lösung praxisrelevanter Probleme anzuwenden.
- professionelle Werkzeuge und Methoden zur Entwicklung interaktiver Nutzerschnittstellen zu nutzen.
- relevante Software-Entwurfsmuster beim Design eigener iOS-Apps anzuwenden.
- geeignete Dienste und Programmierschnittstellen zur Umsetzung vorgegebener Anforderungen an eine mobile App auszuwählen und einzusetzen.
- interaktive iOS-Apps im Rahmen eines nutzerzentrierten Designprozesses zu konzipieren und zu entwickeln.

**Bezüge zu anderen Modulen im Studiengang**

Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Bereich IT & Technik

# Apple Mobile Solution Development I

Kurscode: DLAMSD01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	Für die Teilnahme an diesem Kurs wird ein Mac-Computer (z.B. MacBook, iMac) mit einem aktuellen macOS-Betriebssystem benötigt. Zur App-Entwicklung wird die im Mac-App-Store zur Verfügung gestellte Entwicklungsumgebung Xcode eingesetzt.

## Beschreibung des Kurses

In diesem Kurs erarbeiten sich die Studierenden die Grundlagen zur mobilen App-Entwicklung auf der iOS-Plattform von Apple. Wesentliche Bestandteile dieses Kurses sind das Erlernen und Anwenden von grundlegenden Konzepten der objektorientierten Programmierung mit Swift sowie der Umgang mit professionellen Werkzeugen zum App-Design und zur App-Entwicklung. Anhand von praxisnahen Anwendungsbeispielen gewinnen die Studierenden einen Einblick in die Programmierung und die Entwicklung eigener iOS-Apps.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte und Sprachkonstrukte der Programmiersprache Swift im Kontext eines Programms zu erklären.
- für vorgegebene Aufgabenstellungen einen passenden Algorithmus zu entwickeln und diesen in Form eines Swift-Programmes umzusetzen.
- geeignete Methoden und Werkzeuge zur App-Entwicklung mit Swift einzusetzen.
- den grundlegenden Aufbau einer iOS-App und deren Komponenten zu erläutern.
- eine einfache interaktive iOS-App zu entwickeln.

## Kursinhalt

- In diesem Kurs erarbeiten sich die Studierenden die grundlegenden Konzepte der objektorientierten Programmierung anhand der Programmiersprache Swift. Im Kontext von praktischen Anwendungsbeispielen wenden die Studierenden die erlernten Sprachkonstrukte und Programmiertechniken an und nutzen professionelle Softwareentwicklungswerkzeuge, um eigene Programme zu implementieren, zu debuggen und zu testen. Zudem gewinnen die Studierenden im Rahmen des Kurses einen Einblick in die Entwicklung von iOS-Apps und deren grundlegenden Aufbau. In selbst durchgeführten

Projekten durchlaufen die Studierenden alle Schritte der App-Entwicklung und lernen dadurch den gesamten Entwicklungsprozess von der Konzeption bis zur Veröffentlichung einer iOS-App kennen.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Apple Education (2021): Develop in Swift Explorations. Xcode 12. (URL: <https://books.apple.com/book/id1556366287> [letzter Zugriff: 08.05.2021]).
- Manning, J./Buttfield-Addison, P. (2021): Head First Swift. O'Reilly Media, Inc., Farnham, UK.
- Sillmann, T. (2019): Das Swift Handbuch. Apps programmieren für macOS, iOS, watchOS und tvOS. Hanser, München.
- Swift.org (2021): The Swift Programming Language. Swift 5.4. (URL: <https://docs.swift.org/swift-book/index.html> [letzter Zugriff: 08.05.2021]).

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Projekt
------------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

# Apple Mobile Solution Development II

Kurscode: DLAMSD02

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	Für die Teilnahme an diesem Kurs wird ein Mac-Computer (z.B. MacBook, iMac) mit einem aktuellen macOS-Betriebssystem benötigt. Zur App-Entwicklung wird die im Mac-App-Store zur Verfügung gestellte Entwicklungsumgebung Xcode eingesetzt.

## Beschreibung des Kurses

In diesem Kurs erarbeiten sich die Studierenden fortgeschrittene Prinzipien der mobilen App-Entwicklung auf der iOS-Plattform von Apple. Der Fokus dieses Kurses liegt auf der Entwicklung interaktiver Nutzerschnittstellen unter Verwendung der dafür zur Verfügung stehenden Frameworks und Komponenten. Im Rahmen von eigenen Anwendungsprojekten wenden die Studierenden fortgeschrittene Programmier Techniken an und binden aktuelle Dienste und Schnittstellen zur Umsetzung innovativer App-Funktionen ein. Unter Nutzung moderner Software-Entwicklungswerkzeuge durchlaufen die Studierenden den vollständigen Prozess des Designs, der Implementierung und des Testens von interaktiven iOS-Apps.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- fortgeschrittene Programmier Techniken zur Lösung praxisrelevanter Probleme anzuwenden.
- professionelle Werkzeuge und Methoden zur Entwicklung interaktiver Nutzerschnittstellen zu nutzen.
- relevante Software-Entwurfsmuster beim Design eigener iOS-Apps anzuwenden.
- geeignete Dienste und Programmierschnittstellen zur Umsetzung vorgegebener Anforderungen an eine mobile App auszuwählen und einzusetzen.
- interaktive iOS-Apps im Rahmen eines nutzerzentrierten Designprozesses zu konzipieren und zu entwickeln.

## Kursinhalt

- In dem Kurs erarbeiten sich die Studierenden fortgeschrittene Konzepte der Programmiersprache Swift. Unter Anwendung eines nutzerzentrierten Design- und Entwicklungsprozesses konzipieren und entwickeln die Studierenden interaktive iOS-Apps. Die Studierenden wenden dabei die grundlegenden Prinzipien des Designs interaktiver Nutzerschnittstellen an und nutzen moderne Frameworks und Werkzeuge, um diese umzusetzen. Im Rahmen des Kurses erhalten die Studierenden einen umfassenden Einblick



in die Architektur einer iOS-App. Relevant sind in diesem Zusammenhang auch die Anwendung von gängigen Entwurfsmustern sowie der Prinzipien der ereignisgesteuerten Programmierung. Im Kontext eigener Anwendungsprojekte machen sich die Studierenden mit dem Umgang und der Einbindung von externen Diensten und Programmierschnittstellen vertraut, die zur Umsetzung spezieller App-Funktionen bereitstehen.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Apple Education (2021): Develop in Swift Fundamentals. Xcode 12. (URL: <https://books.apple.com/book/id1556365994> [letzter Zugriff: 08.05.2021]).
- Apple Education (2021): Develop in Swift Data Collections. Xcode 12. (URL: <https://books.apple.com/book/id1556365920> [letzter Zugriff: 08.05.2021]).
- Sillmann, T. (2019): Das Swift Handbuch. Apps programmieren für macOS, iOS, watchOS und tvOS. Hanser, München.
- Swift.org (2021): The Swift Programming Language. Swift 5.4. (URL: <https://docs.swift.org/swift-book/index.html> [letzter Zugriff: 08.05.2021]).

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Projekt
-----------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Folien

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Projekt
------------------------------------	---------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Projektbericht

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
120 h	0 h	30 h	0 h	0 h	150 h

<b>Lehrmethoden</b>	
<input type="checkbox"/> Learning Sprints®	<input type="checkbox"/> Repetitorium
<input type="checkbox"/> Skript	<input type="checkbox"/> Creative Lab
<input type="checkbox"/> Vodcast	<input checked="" type="checkbox"/> Prüfungsleitfaden
<input type="checkbox"/> Shortcast	<input type="checkbox"/> Live Tutorium/Course Feed
<input type="checkbox"/> Audio	<input type="checkbox"/> Reader
<input type="checkbox"/> Musterklausur	<input checked="" type="checkbox"/> Folien

DLAMSD02

## Studium Generale

Modulcode: DLBSG

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> keine	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	--	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

N.N. (Studium Generale I) / N.N. (Studium Generale II)

### Kurse im Modul

- Studium Generale I (DLBSG01)
- Studium Generale II (DLBSG02)

### Art der Prüfung(en)

#### Modulprüfung

#### Teilmodulprüfung

##### Studium Generale I

- Studienformat "Fernstudium": Siehe gewählter Kurs
- Studienformat "myStudium": Siehe gewählter Kurs

##### Studium Generale II

- Studienformat "Kombistudium": Siehe gewählter Kurs
- Studienformat "Fernstudium": Siehe gewählter Kurs
- Studienformat "myStudium": Siehe gewählter Kurs

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****Studium Generale I**

Als Kurs für das „Studium Generale“ sind prinzipiell alle IU-Bachelorkurse anrechenbar, sodass inhaltlich aus der gesamten Breite des IU Fernstudiums gewählt werden kann.

**Studium Generale II**

Als Kurs für das „Studium Generale“ sind prinzipiell alle IU-Bachelorkurse anrechenbar, sodass inhaltlich aus der gesamten Breite des IU Fernstudiums gewählt werden kann.

**Qualifikationsziele des Moduls****Studium Generale I**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- erworbene Schlüsselkompetenzen auf Fragestellungen ihres Studienfaches und/oder in ihrem beruflichen Umfeld anzuwenden.
- eigene Fähig- und Fertigkeiten selbstgesteuert zu vertiefen.
- über die Grenzen ihres eigenen Fachgebietes hinauszublicken.

**Studium Generale II**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- erworbene Schlüsselkompetenzen auf Fragestellungen ihres Studienfaches und/oder in ihrem beruflichen Umfeld anzuwenden.
- eigene Fähig- und Fertigkeiten selbstgesteuert zu vertiefen.
- über die Grenzen ihres eigenen Fachgebietes hinauszublicken.

**Bezüge zu anderen Modulen im Studiengang**

Ist ein eigenständiges Angebot mit möglichen Bezügen zu verschiedenen Pflicht- und Wahlpflichtmodulen

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme des IU Fernstudiums

# Studium Generale I

Kurscode: DLBSG01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

## Beschreibung des Kurses

Im Rahmen des Kurses „Studium Generale I“ vertiefen die Studierenden ihr Wissen in einem selbstgewählten Themenfeld durch das Absolvieren eines IU-Kurses außerhalb ihres geltenden Curriculums. Sie haben dadurch die Möglichkeit, über den Tellerand ihres eigenen Fachgebietes hinauszublicken und weitere (Schlüssel-)Kompetenzen zu erwerben. Die damit verbundene Wahlmöglichkeit versetzt die Studierenden in die Lage, ihre Studieninhalte selbstbestimmt noch stärker auf für sie relevante Fragestellungen hin auszurichten und/oder ausgewählte Kompetenzen zu stärken oder zu entwickeln.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- erworbene Schlüsselkompetenzen auf Fragestellungen ihres Studienfaches und/oder in ihrem beruflichen Umfeld anzuwenden.
- eigene Fähig- und Fertigkeiten selbstgesteuert zu vertiefen.
- über die Grenzen ihres eigenen Fachgebietes hinauszublicken.

## Kursinhalt

- Der Kurs „Studium Generale I“ bietet den Studierenden die Möglichkeit, dass sie Lehrveranstaltungen außerhalb ihres Curriculums absolvieren und sich das Ergebnis als Wahlpflichtfach anerkennen lassen können. Hierfür sind prinzipiell alle IU-Bachelorkurse anrechenbar sowie akademische Leistungen anderer staatlich anerkannter Hochschulen, die die folgenden Voraussetzungen erfüllen:
  - Sie sind nicht integraler Bestandteil des geltenden Pflichtcurriculums.
  - Sie haben keine Zugangsvoraussetzungen oder die Studierenden können die Erfüllung der Zugangsvoraussetzung nachweisen.
- Die Prüfung der gewählten Kurse muss zur Anerkennung als Teil des ‚Studium Generale‘ vollumfänglich abgelegt und endgültig bestanden sein.

<b>Literatur</b>
<b>Pflichtliteratur</b>
<b>Weiterführende Literatur</b> <ul style="list-style-type: none"><li>▪ Siehe Kursbeschreibung des gewählten Kurses</li></ul>



**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Siehe gewählter Kurs
-----------------------------------	--

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Siehe gewählter Kurs

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
0 h	0 h	0 h	0 h	0 h	0 h

<b>Lehrmethoden</b>
Siehe Kursbeschreibung des gewählten Kurses

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Siehe gewählter Kurs
---------------------------------	--

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Siehe gewählter Kurs

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
0 h	0 h	0 h	0 h	0 h	0 h

<b>Lehrmethoden</b>
Siehe Kursbeschreibung des gewählten Kurses

## Studium Generale II

Kurscode: DLBSG02

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

### Beschreibung des Kurses

Im Rahmen des Kurses „Studium Generale II“ vertiefen die Studierenden ihr Wissen in einem selbstgewählten Themenfeld durch das Absolvieren eines IU-Kurses außerhalb ihres geltenden Curriculums. Sie haben dadurch die Möglichkeit, über den Tellerand ihres eigenen Fachgebietes hinauszublicken und weitere (Schlüssel-)Kompetenzen zu erwerben. Die damit verbundene Wahlmöglichkeit versetzt die Studierenden in die Lage, ihre Studieninhalte selbstbestimmt noch stärker auf für sie relevante Fragestellungen hin auszurichten und/oder ausgewählte Kompetenzen zu stärken oder zu entwickeln.

### Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- erworbene Schlüsselkompetenzen auf Fragestellungen ihres Studienfaches und/oder in ihrem beruflichen Umfeld anzuwenden.
- eigene Fähig- und Fertigkeiten selbstgesteuert zu vertiefen.
- über die Grenzen ihres eigenen Fachgebietes hinauszublicken.

### Kursinhalt

- Der Kurs „Studium Generale II“ bietet den Studierenden die Möglichkeit, dass sie Lehrveranstaltungen außerhalb ihres Curriculums absolvieren und sich das Ergebnis als Wahlpflichtfach anerkennen lassen können. Hierfür sind prinzipiell alle IU-Bachelorkurse anrechenbar sowie akademische Leistungen anderer staatlich anerkannter Hochschulen, die die folgenden Voraussetzungen erfüllen:
  - Sie sind nicht integraler Bestandteil des geltenden Pflichtcurriculums.
  - Sie haben keine Zugangsvoraussetzungen oder die Studierenden können die Erfüllung der Zugangsvoraussetzung nachweisen.
- Die Prüfung der gewählten Kurse muss zur Anerkennung als Teil des ‚Studium Generale‘ vollumfänglich abgelegt und endgültig bestanden sein.

<b>Literatur</b>
<b>Pflichtliteratur</b>
<b>Weiterführende Literatur</b> <ul style="list-style-type: none"><li>▪ Siehe Kursbeschreibung des gewählten Kurses</li></ul>

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Siehe gewählter Kurs
------------------------------------	--

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Siehe gewählter Kurs

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
0 h	0 h	0 h	0 h	0 h	0 h

<b>Lehrmethoden</b>
Siehe Kursbeschreibung des gewählten Kurses

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Siehe gewählter Kurs
-----------------------------------	--

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Siehe gewählter Kurs

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
0 h	0 h	0 h	0 h	0 h	0 h

<b>Lehrmethoden</b>
Siehe Kursbeschreibung des gewählten Kurses

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Siehe gewählter Kurs
---------------------------------	--

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Siehe gewählter Kurs

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
0 h	0 h	0 h	0 h	0 h	0 h

<b>Lehrmethoden</b>
Siehe Kursbeschreibung des gewählten Kurses

DLBSG02



## Bachelorarbeit

Modulcode: BBAK

<b>Modultyp</b> s. Curriculum	<b>Zugangsvoraussetzungen</b> gemäß Studien- und Prüfungsordnung	<b>Niveau</b> BA	<b>ECTS</b> 10	<b>Zeitaufwand Studierende</b> 300 h
----------------------------------	---	---------------------	-------------------	---

<b>Semester</b> s. Curriculum	<b>Dauer</b> Minimaldauer: 1 Semester	<b>Regulär angeboten im</b> WiSe/SoSe	<b>Kurs- und Prüfungssprache</b> Deutsch
----------------------------------	---	--	---

### Modulverantwortliche(r)

Studiengangleiter (SGL) (Bachelorarbeit) / Studiengangsleiter (SGL) (Kolloquium)

### Kurse im Modul

- Bachelorarbeit (BBAK01)
- Kolloquium (BBAK02)

### Art der Prüfung(en)

#### Modulprüfung

#### Teilmodulprüfung

##### Bachelorarbeit

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Bachelorarbeit
- Studienformat "myStudium": Schriftliche Ausarbeitung: Bachelorarbeit
- Studienformat "Kombistudium": Schriftliche Ausarbeitung: Bachelorarbeit

##### Kolloquium

- Studienformat "myStudium": Kolloquium
- Studienformat "Fernstudium": Kolloquium
- Studienformat "Kombistudium": Kolloquium

### Anteil der Modulnote an der Gesamtnote

s. Curriculum

**Lehrinhalt des Moduls****Bachelorarbeit**

- Bachelorarbeit

**Kolloquium**

- Kolloquium zur Bachelorarbeit

**Qualifikationsziele des Moduls****Bachelorarbeit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Anwendung der fachlichen und methodischen Kompetenzen, die sie im Studium erworben haben, zu bearbeiten.
- eigenständig – unter fachlich-methodischer Anleitung eines akademischen Betreuers – ausgewählte Aufgabenstellungen mit wissenschaftlichen Methoden zu analysieren, kritisch zu bewerten sowie entsprechende Lösungsvorschläge zu erarbeiten.
- eine dem Thema der Bachelorarbeit angemessene Erfassung und Analyse vorhandener (Forschungs-)Literatur vorzunehmen.
- eine ausführliche schriftliche Ausarbeitung unter Einhaltung wissenschaftlicher Methoden zu erstellen.

**Kolloquium**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Beachtung akademischer Präsentations- und Kommunikationstechniken vorzustellen.
- das in der Bachelorarbeit gewählte wissenschaftliche und methodische Vorgehen reflektiert darzustellen.
- themenbezogene Fragen der Fachexperten (Gutachter der Bachelorarbeit) aktiv zu beantworten.

**Bezüge zu anderen Modulen im Studiengang**

Alle Module

**Bezüge zu anderen Studiengängen der Hochschule**

Alle Bachelor-Programme im Fernstudium

# Bachelorarbeit

Kurscode: BBAK01

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		9	gemäß Studien- und Prüfungsordnung

## Beschreibung des Kurses

Ziel und Zweck der Bachelorarbeit ist es, die im Verlauf des Studiums erworbenen fachlichen und methodischen Kompetenzen in Form einer akademischen Abschlussarbeit mit thematischem Bezug zum Studienschwerpunkt erfolgreich anzuwenden. Inhalt der Bachelorarbeit kann eine praktisch-empirische oder aber theoretisch-wissenschaftliche Problemstellung sein. Studierende sollen unter Beweis stellen, dass sie eigenständig unter fachlich-methodischer Anleitung eines akademischen Betreuers eine ausgewählte Problemstellung mit wissenschaftlichen Methoden analysieren, kritisch bewerten und Lösungsvorschläge erarbeiten können. Das von dem Studierenden zu wählende Thema aus dem jeweiligen Studienschwerpunkt soll nicht nur die erworbenen wissenschaftlichen Kompetenzen unter Beweis stellen, sondern auch das akademische Wissen des Studierenden vertiefen und abrunden, um seine Berufsfähigkeiten und -fertigkeiten optimal auf die Bedürfnisse des zukünftigen Tätigkeitsfeldes auszurichten.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Anwendung der fachlichen und methodischen Kompetenzen, die sie im Studium erworben haben, zu bearbeiten.
- eigenständig – unter fachlich-methodischer Anleitung eines akademischen Betreuers – ausgewählte Aufgabenstellungen mit wissenschaftlichen Methoden zu analysieren, kritisch zu bewerten sowie entsprechende Lösungsvorschläge zu erarbeiten.
- eine dem Thema der Bachelorarbeit angemessene Erfassung und Analyse vorhandener (Forschungs-)Literatur vorzunehmen.
- eine ausführliche schriftliche Ausarbeitung unter Einhaltung wissenschaftlicher Methoden zu erstellen.

## Kursinhalt

- Die Bachelorarbeit muss zu einer Themenstellung geschrieben werden, die einen inhaltlichen Bezug zum jeweiligen Studienschwerpunkt aufweist. Im Rahmen der Bachelorarbeit müssen die Problemstellung sowie das wissenschaftliche Untersuchungsziel klar herausgestellt werden. Die Arbeit muss über eine angemessene Literaturanalyse den aktuellen Wissensstand des zu untersuchenden Themas widerspiegeln. Der Studierende muss seine Fähigkeit unter Beweis stellen, das erarbeitete Wissen in Form einer eigenständigen und problemlösungsorientierten Anwendung theoretisch und/oder empirisch zu verwerten.

**Literatur**

**Pflichtliteratur**

**Weiterführende Literatur**

- Hunziker, A.W. (2010): Spaß am wissenschaftlichen Arbeiten. So schreiben Sie eine gute Semester-, Bachelor- oder Masterarbeit. 4. Auflage, Verlag SKV, Zürich.
- Wehrlin, U. (2010): Wissenschaftliches Arbeiten und Schreiben. Leitfaden zur Erstellung von Bachelorarbeit, Masterarbeit und Dissertation – von der Recherche bis zur Buchveröffentlichung. AVM, München.
- Themenabhängige Literaturlauswahl

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Thesis-Kurs
-----------------------------------	-------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Bachelorarbeit

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
270 h	0 h	0 h	0 h	0 h	270 h

<b>Lehrmethoden</b>
Selbstständige Projektbearbeitung unter akademischer Anleitung.

**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Thesis-Kurs
---------------------------------	-------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Bachelorarbeit

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
270 h	0 h	0 h	0 h	0 h	270 h

<b>Lehrmethoden</b>
Selbstständige Projektbearbeitung unter akademischer Anleitung.

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Thesis-Kurs
------------------------------------	-------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung: Bachelorarbeit

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
270 h	0 h	0 h	0 h	0 h	270 h

<b>Lehrmethoden</b>
Selbstständige Projektbearbeitung unter akademischer Anleitung.

# Kolloquium

Kurscode: BBAK02

Niveau	Kurs- und Prüfungssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		1	Gemäß Studien- und Prüfungsordnung

## Beschreibung des Kurses

Das Kolloquium wird nach Einreichung der Bachelorarbeit durchgeführt. Es erfolgt auf Einladung der Gutachter. Im Rahmen des Kolloquiums müssen die Studierenden unter Beweis stellen, dass sie den Inhalt und die Ergebnisse der schriftlichen Arbeit in vollem Umfang eigenständig erbracht haben. Inhalt des Kolloquiums ist eine Präsentation der wichtigsten Arbeitsinhalte und Untersuchungsergebnisse durch den Studierenden sowie die Beantwortung von Fragen der Gutachter.

## Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Beachtung akademischer Präsentations- und Kommunikationstechniken vorzustellen.
- das in der Bachelorarbeit gewählte wissenschaftliche und methodische Vorgehen reflektiert darzustellen.
- themenbezogene Fragen der Fachexperten (Gutachter der Bachelorarbeit) aktiv zu beantworten.

## Kursinhalt

1. Das Kolloquium umfasst eine Präsentation der wichtigsten Ergebnisse der Bachelorarbeit, gefolgt von der Beantwortung von Fachfragen der Gutachter durch den Studierenden.

## Literatur

### Pflichtliteratur

### Weiterführende Literatur

- Renz, K.-C. (2016): Das 1 x 1 der Präsentation. Für Schule, Studium und Beruf. 2. Auflage, Springer Gabler, Wiesbaden.



**Studienformat myStudium**

<b>Studienform</b> myStudium	<b>Kursart</b> Kolloquium
---------------------------------	------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Kolloquium

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
30 h	0 h	0 h	0 h	0 h	30 h

<b>Lehrmethoden</b>
Moderne Präsentationstechnologien stehen zur Verfügung

**Studienformat Fernstudium**

<b>Studienform</b> Fernstudium	<b>Kursart</b> Kolloquium
-----------------------------------	------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Kolloquium

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
30 h	0 h	0 h	0 h	0 h	30 h

<b>Lehrmethoden</b>
Moderne Präsentationstechnologien stehen zur Verfügung

**Studienformat Kombistudium**

<b>Studienform</b> Kombistudium	<b>Kursart</b> Kolloquium
------------------------------------	------------------------------

<b>Informationen zur Prüfung</b>	
<b>Prüfungszulassungsvoraussetzungen</b>	<b>BOLK:</b> Nein
<b>Prüfungsleistung</b>	Kolloquium

<b>Zeitaufwand Studierende</b>					
<b>Selbststudium</b>	<b>Präsenzstudium</b>	<b>Tutorium</b>	<b>Selbstüberprüfung</b>	<b>Praxisanteil</b>	<b>Gesamt</b>
30 h	0 h	0 h	0 h	0 h	30 h

<b>Lehrmethoden</b>
Moderne Präsentationstechnologien stehen zur Verfügung