MODULHANDBUCH

Bachelor of Science

Bachelor Cyber Security (FS-BACSD)

180 CP

Fernstudium

Stand: 28.Mai 2025

INTERNATIONALE HOCHSCHULE

Klassifizierung: Grundständig

Inhaltsverzeichnis

1. Semester

Modul DLBIBRVS: Betriebssysteme, Rechnernetze und verteilte Systeme
Modulbeschreibung 12
Kurs DLBIBRVS01: Betriebssysteme, Rechnernetze und verteilte Systeme 14

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 36
Kurs DLBWIRITT01: Einführung in das wissenschaftliche Arbeiten für IT und Technik 38

Modul DLBDSIPWP_D: Einführung in die Programmierung mit Python
Modulbeschreibung 44
Kurs DLBDSIPWP01_D: Einführung in die Programmierung mit Python 46

Modul DLBDSSPDS_D: Statistik - Wahrscheinlichkeit und deskriptive Statistik
Modulbeschreibung 51
Kurs DLBDSSPDS01_D: Statistik - Wahrscheinlichkeit und deskriptive Statistik 53

2. Semester

Modul DLBINGOPJ-01: Grundlagen der objektorientierten Programmierung mit Java
Modulbeschreibung 59
Kurs DLBCSOOPJ01_D: 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 75
Kurs DLBKA01: Kollaboratives Arbeiten 77

Modul DLBCSEINF_D: Einführung in die Netzwerkforensik
Modulbeschreibung 84
Kurs DLBCSEINF01_D: Einführung in die Netzwerkforensik 86

Modul IREN: Requirements Engineering
Modulbeschreibung 92
Kurs IREN01: Requirements Engineering 94

Modul DLBCSESPB_D: Grundzüge des System-Pentestings
Modulbeschreibung 101
Kurs DLBCSESPB01_D: Grundzüge des System-Pentestings 103

---

3. Semester

Modul DLBIHK: Interkulturelle und ethische Handlungskompetenzen
Modulbeschreibung 110
Kurs DLBIHK01: Interkulturelle und ethische Handlungskompetenzen 112

Modul DLBINGEIT: Einführung in das Internet of Things
Modulbeschreibung 118
Kurs DLBINGEIT01: Einführung in das Internet of Things 120

Modul DLBIADPS-01: Algorithmen, Datenstrukturen und Programmiersprachen
Modulbeschreibung 127
Kurs DLBIADPS01-01: Algorithmen, Datenstrukturen und Programmiersprachen 129

Modul DLBITIML: Theoretische Informatik und Mathematische Logik
Modulbeschreibung 135
Kurs DLBITIML01: Theoretische Informatik und Mathematische Logik 137

Modul IPMG-01: IT-Projektmanagement
Modulbeschreibung 144
Kurs IPMG01-01: IT-Projektmanagement 146

Modul DLBCSEDCSW_D: DevSecOps und gängige Software-Schwachstellen
Modulbeschreibung 152
Kurs DLBCSEDCSW01_D: DevSecOps und gängige Software-Schwachstellen 154

---

4. Semester

Modul DLBCSITSM1-01_D: IT-Servicemanagement
Modulbeschreibung 161
Kurs DLBCSITSM01-01_D: IT-Servicemanagement 163

Modul DLBISIC2-01: Kryptografische Verfahren
Modulbeschreibung 169
Kurs DLBISIC02-01: Kryptografische Verfahren 171

Modul DLBIITR-01: IT-Recht
Modulbeschreibung 178
Kurs DLBIITR01-01: IT-Recht 180

Modul DLBCSEHSF_D: Host- und Softwareforensik
Modulbeschreibung 188
Kurs DLBCSEHSF01_D: Host- und Softwareforensik 190

Modul DLBDSEAIS1_D: Artificial Intelligence
Modulbeschreibung 196
Kurs DLBDSEAIS01_D: Artificial Intelligence 198

Modul DLBCSEISS_D: Standards der Informationssicherheit
Modulbeschreibung 204
Kurs DLBCSEISS01_D: Standards der Informationssicherheit 206

---

5. Semester

Modul DLBCSSCTCS_D: Seminar: Aktuelle Themen in Computer Science
Modulbeschreibung 212
Kurs DLBCSSCTCS01_D: Seminar: Aktuelle Themen in Computer Science 214

Modul DLBDSEDA1_D: Advanced Data Analysis
Modulbeschreibung 219
Kurs DLBDSEDA01_D: Advanced Data Analysis 221

Modul DLBDSEDA2_D: Projekt: Datenanalyse
Modulbeschreibung 226
Kurs DLBDSEDA02_D: Projekt: Datenanalyse 228

Modul DLBDSCC_D: Cloud Computing
Modulbeschreibung 233
Kurs DLBDSCC01_D: Cloud Computing 235

Modul DLBCSEEISC_D: IT-Sicherheitsberatung
Modulbeschreibung 240
Kurs DLBCSEEISC01_D: Technische und betriebliche IT-Sicherheitskonzeptionen 243
Kurs DLBCSEEISC02_D: Projekt: Einsatz und Konfiguration von SIEM-Systemen 249

Modul DLBCSEESE_D: Social Engineering

Modulbeschreibung 254
Kurs DLBCSEESE01_D: Social Engineering und Insider Threats 257
Kurs DLBCSEESE02_D: Projekt: Social Engineering 263

Modul DLBCSEEHF_E: Host Forensics
Modulbeschreibung 269
Kurs DLBCSEEHF01_E: Static and Dynamic Malware Analysis 271
Kurs DLBCSEEHF02_E: Seminar: Sandbox Interpretation 276

Modul DLBCSEEDSO-01_D: DevSecOps
Modulbeschreibung 280
Kurs DLBWIWTMAS01: Techniken und Methoden der agilen Softwareentwicklung 283
Kurs DLBCSEEDSO01_D: Projekt: Agiles DevSecOps-Software-Engineering 289

Modul DLBCSEESCN_D: Sicherheit in komplexen Netzwerken
Modulbeschreibung 293
Kurs IAMG01: IT-Architekturmanagement 295
Kurs DLBCSEESCN01_D: Projekt: IT-Sicherheitsarchitekturen 300

Modul DLBCSEENF_E: Network Forensics
Modulbeschreibung 304
Kurs DLBCSEENF01_E: Protocols, Log- and Dataflow-Analysis in Depth 306
Kurs DLBCSEENF02_E: Seminar: Threat Hunting, Analysis and Incident Response 311

Modul DLBSG: Studium Generale I und II
Modulbeschreibung 315
Kurs DLBSG01: Studium Generale I 317
Kurs DLBSG02: Studium Generale II 322

---

6. Semester

Modul IWBI: Business Intelligence
Modulbeschreibung 329
Kurs IWBI01: Business Intelligence 332
Kurs IWBI02: Projekt: Business Intelligence 339

Modul DLBCSEEFT_D: Future Threats
Modulbeschreibung 344
Kurs DLBCSEEFT01_D: Threat Modeling 347
Kurs DLBCSEEFT02_D: Projekt: Threat Modeling 352

Modul DLBCSEECS_E: Cloud Security
Modulbeschreibung 357
Kurs DLBCSEECS01_E: Security Controls in the Cloud 359

Kurs DLBCSEECS02_E: Project: Security by Design in the Cloud 364

Modul DLBCSEEPT_E: Vulnerability Analysis and Pentesting
Modulbeschreibung 368
Kurs DLBCSEEPT01_E: Principles of Ethical Hacking 370
Kurs DLBCSEEPT02_E: Project: Pentesting 376

Modul DLBCSEEIST_D: Industrielle Systemsicherheit
Modulbeschreibung 379
Kurs IGIS01: Grundlagen der industriellen Softwaretechnik 382
Kurs DLBCSEEIST01_D: Sicherheit im Internet of Things 387

Modul DLBCSEECTI_E: Cyber Threat Intelligence
Modulbeschreibung 391
Kurs DLBCSEECTI01_E: Attack Models and Threat Feeds 394
Kurs DLBCSEECTI02_E: Project: Defense against APTs 400

Modul DLBCSEEMT_D: Telekommunikationsspezifische Bedrohungen
Modulbeschreibung 405
Kurs DLBCSEEMT01_D: Funk- und Telekommunikationssicherheit 408
Kurs DLBCSEEMT02_D: Softwarearchitektur mobiler Geräte 413

Modul DLAMSD: Apple Mobile Solution Development
Modulbeschreibung 418
Kurs DLAMSD01: Apple Mobile Solution Development I 421
Kurs DLAMSD02: Apple Mobile Solution Development II 426

Modul DLBSGDUV: Studium Generale III und IV
Modulbeschreibung 431
Kurs DLBSG03: Studium Generale III 433
Kurs DLBSG04: Studium Generale IV 437

Modul DLBCSEEISC_D: IT-Sicherheitsberatung
Modulbeschreibung 441
Kurs DLBCSEEISC01_D: Technische und betriebliche IT-Sicherheitskonzeptionen 444
Kurs DLBCSEEISC02_D: Projekt: Einsatz und Konfiguration von SIEM-Systemen 450

Modul DLBCSEESE_D: Social Engineering
Modulbeschreibung 455
Kurs DLBCSEESE01_D: Social Engineering und Insider Threats 458
Kurs DLBCSEESE02_D: Projekt: Social Engineering 464

Modul DLBCSEEHF_E: Host Forensics
Modulbeschreibung 470
Kurs DLBCSEEHF01_E: Static and Dynamic Malware Analysis 472

Kurs DLBCSEEHF02_E: Seminar: Sandbox Interpretation 477

Modul DLBCSEEDSO-01_D: DevSecOps
Modulbeschreibung 481
Kurs DLBWIWTMAS01: Techniken und Methoden der agilen Softwareentwicklung 484
Kurs DLBCSEEDSO01_D: Projekt: Agiles DevSecOps-Software-Engineering 490

Modul DLBCSEESCN_D: Sicherheit in komplexen Netzwerken
Modulbeschreibung 494
Kurs IAMG01: IT-Architekturmanagement 496
Kurs DLBCSEESCN01_D: Projekt: IT-Sicherheitsarchitekturen 501

Modul DLBCSEENF_E: Network Forensics
Modulbeschreibung 505
Kurs DLBCSEENF01_E: Protocols, Log- and Dataflow-Analysis in Depth 507
Kurs DLBCSEENF02_E: Seminar: Threat Hunting, Analysis and Incident Response 512

Modul IWBI: Business Intelligence
Modulbeschreibung 516
Kurs IWBI01: Business Intelligence 519
Kurs IWBI02: Projekt: Business Intelligence 526

Modul DLBCSEEFT_D: Future Threats
Modulbeschreibung 531
Kurs DLBCSEEFT01_D: Threat Modeling 534
Kurs DLBCSEEFT02_D: Projekt: Threat Modeling 539

Modul DLBCSEECS_E: Cloud Security
Modulbeschreibung 544
Kurs DLBCSEECS01_E: Security Controls in the Cloud 546
Kurs DLBCSEECS02_E: Project: Security by Design in the Cloud 551

Modul DLBCSEEPT_E: Vulnerability Analysis and Pentesting
Modulbeschreibung 555
Kurs DLBCSEEPT01_E: Principles of Ethical Hacking 557
Kurs DLBCSEEPT02_E: Project: Pentesting 563

Modul DLBCSEEIST_D: Industrielle Systemsicherheit
Modulbeschreibung 566
Kurs IGIS01: Grundlagen der industriellen Softwaretechnik 569
Kurs DLBCSEEIST01_D: Sicherheit im Internet of Things 574

Modul DLBCSEECTI_E: Cyber Threat Intelligence
Modulbeschreibung 578
Kurs DLBCSEECTI01_E: Attack Models and Threat Feeds 581

Kurs DLBCSEECTI02_E: Project: Defense against APTs 587

Modul DLBCSEEMT_D: Telekommunikationsspezifische Bedrohungen
Modulbeschreibung 592
Kurs DLBCSEEMT01_D: Funk- und Telekommunikationssicherheit 595
Kurs DLBCSEEMT02_D: Softwarearchitektur mobiler Geräte 600

Modul BWSC: Supply Chain Management
Modulbeschreibung 605
Kurs BWSC01: Supply-Chain-Management I 609
Kurs BWSC02: Supply-Chain-Management II 616

Modul DLBINGASF: Angewandte Smart Factory
Modulbeschreibung 623
Kurs DLBINGSF01: Smart Factory 625
Kurs DLBINGPSDF01: Projekt: Smart Devices & Factory 630

Modul DLBCSDWRA: Robotics und Automatisierung
Modulbeschreibung 633
Kurs DLBINGFVI01: Fertigungsverfahren Industrie 4.0 636
Kurs DLBINGAUR01: Automatisierung und Robotics 643

Modul DLBCSEMSE_D: Mobile Software Engineering
Modulbeschreibung 650
Kurs DLBCSEMSE01_D: Mobile Software Engineering 653
Kurs DLBCSEMSE02_D: Projekt: Mobile Software Engineering 658

Modul DLAMSD: Apple Mobile Solution Development
Modulbeschreibung 663
Kurs DLAMSD01: Apple Mobile Solution Development I 666
Kurs DLAMSD02: Apple Mobile Solution Development II 671

Modul DLBMSERP: Microsoft ERP- Dynamics 365 Business Central - Functional Consultant
Modulbeschreibung 676
Kurs DLBMSERP01: Project: Dynamics 365 Business Central - Financial Company Setup 679
Kurs DLBMSERP02: Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution 684

Modul DLBSAPBPI: SAP - SAP S/4HANA Business Process Integration - Application Associate
Modulbeschreibung 689
Kurs DLBSAPBPI01: Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management 692
Kurs DLBSAPBPI02: Project: SAP S/4HANA - Business Processes 697

Modul DLBKAENT: Karriere-Entwicklung

Modulbeschreibung 702
Kurs DLBKAENT01: Persönlicher Karriereplan 705
Kurs DLBKAENT02: Persönlicher Elevator Pitch 711

Modul DLBAWSCLSP: AWS Cloud Specialization
Modulbeschreibung 716
Kurs DLBPAWSCLES01: Project: AWS - Cloud Essentials 719
Kurs DLBPAWSCLAD01: Project: AWS - Cloud Advanced 724

Modul DLBEAIPTPICOP: AI Prompting Techniques and Process Innovation with Copilot
Modulbeschreibung 730
Kurs DLBPKIEKPT01_E: Project: AI Excellence with Creative Prompting Techniques 733
Kurs DLBPPICOP01: Project: Process Innovation with Copilot 738

Modul DLBSGFUS: Studium Generale V und VI
Modulbeschreibung 741
Kurs DLBSG05: Studium Generale V 743
Kurs DLBSG06: Studium Generale VI 746

Modul BBAK: Bachelorarbeit
Modulbeschreibung 749
Kurs BBAK01: Bachelorarbeit 752
Kurs BBAK02: Kolloquium 759

1. Semester

Betriebssysteme, Rechnernetze und verteilte Systeme

Modulcode: DLBIBRVS

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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)

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

Kurse im Modul

- Betriebssysteme, Rechnernetze und verteilte Systeme (DLBIBRVS01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: myStudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Betriebssysteme, Rechnernetze und verteilte Systeme

Kurscode: DLBIBRVS01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Aufl.). Vieweg+Teubner. ▪ Gumm, H. P., & Sommer, M. (2013). *Einführung in die Informatik* (10. Aufl.). Oldenbourg. ▪ Luntovskyy, A., & Gütter, D. (2023). *Moderne Rechnernetze* (2. Aufl.). Springer Vieweg. ▪ Mandl, P. (2020). *Grundkurs Betriebssysteme* (5. Aufl.). Springer Vieweg. ▪ Schill, A., & Springer, T. (2012). *Verteilte Systeme* (2. Aufl.). Springer Vieweg. ▪ Tanenbaum, A. S., & Bos, H. (2016). *Moderne Betriebssysteme* (4. Aufl.). Pearson Deutschland. ▪ Tanenbaum, A. S., Feamster, N., & Wetherall, D. J. (2024). *Computernetzwerke* (6. Aufl.). Pearson Deutschland.

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	30 h	0 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Einführung in Datenschutz und IT-Sicherheit

Modulcode: DLBINGEDS

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Ralf Kneuper (Einführung in Datenschutz und IT-Sicherheit)

Kurse im Modul

- Einführung in Datenschutz und IT-Sicherheit (DLBISIC01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: myStudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Einführung in Datenschutz und IT-Sicherheit

Kurscode: DLBISIC01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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-Verbünden
   - 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

- Eckert, C. (2018). IT-Sicherheit: Konzepte – Verfahren – Protokolle (10. Aufl.). Oldenbourg Wissenschaftsverlag.
- Frankenstein, R. (2023). BSI IT-Grundschutz – Arbeitswerkzeug für ganzheitliche Informationssicherheit. Datenschutz und Datensicherheit, 47, 410–415.
- Kersken, S. (2021). IT-Handbuch für Fachinformatiker: Der Ausbildungsbegleiter (10. Aufl.). Rheinwerk.
- Kneuper, R. (2021). Datenschutz für Softwareentwicklung und IT. Springer Vieweg.
- Maseberg, S. (2023). KRITIS-Regularien. Datenschutz und Datensicherheit, 47, 541–544.

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Mathematik: Analysis

Modulcode: DLBBIMD

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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	Teilmodulprüfung
Studienformat: myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für weitere Module im Bereich Methoden	Alle Bachelor-Programme im Bereich Wirtschaft & Management

Mathematik: Analysis

Kurscode: DLBBIMD01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

Pflichtliteratur

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 myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
	☑ Audio	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
	☑ Audio	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
	☑ Audio	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Einführung in das wissenschaftliche Arbeiten für IT und Technik

Modulcode: DLBWIRITT

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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	Teilmodulprüfung
Studienformat: Duales myStudium Advanced Workbook Studienformat: Duales Studium Advanced Workbook Studienformat: myStudium Advanced Workbook Studienformat: Fernstudium Advanced Workbook	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Methoden	Alle Bachelor-Programme im Bereich Wirtschaft

Einführung in das wissenschaftliche Arbeiten für IT und Technik

Kurscode: DLBWIRITT01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
	☑ Folien	

Studienformat Duales Studium

Studienform	Kursart
Duales Studium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium/ synchrone virtuelle Lehre**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
129,75 h	13,5 h	6,75 h	0 h	0 h	150 h

Lehrmethoden
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

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Einführung in die Programmierung mit Python

Modulcode: DLBDSIPWP_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. 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	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module im Bereich Data Science & Artificial Intelligence	Alle Bachelor-Programme im Bereich IT & Technik

Einführung in die Programmierung mit Python

Kurscode: DLBDSIPWP01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Statistik - Wahrscheinlichkeit und deskriptive Statistik

Modulcode: DLBDSSPDS_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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 (Statistik - Wahrscheinlichkeit und deskriptive Statistik)

Kurse im Modul

- Statistik - Wahrscheinlichkeit und deskriptive Statistik (DLBDSSPDS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur oder Advanced Workbook, 90 Minuten Studienformat: myStudium Klausur oder Advanced Workbook, 90 Minuten Studienformat: Duales myStudium Klausur oder Advanced Workbook, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Methoden	Alle Bachelor-Programme im Bereich Wirtschaft

Statistik - Wahrscheinlichkeit und deskriptive Statistik

Kurscode: DLBDSSPDS01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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- undSozialwissenschaftler (18. Aufl.). De Gruyter Studium.
- Mathai, A. M. & Haubold, H. J. (2018). Probability and Statistics: a Course for Physicists andEngineers. 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

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Advanced Workbook, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
	☑ Audio	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Advanced Workbook, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
	☑ Audio	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Advanced Workbook, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
	☑ Audio	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

2. Semester

Grundlagen der objektorientierten Programmierung mit Java

Modulcode: DLBINGOPJ-01

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Cornelia Heinisch (Grundlagen der objektorientierten Programmierung mit Java)

Kurse im Modul

- Grundlagen der objektorientierten Programmierung mit Java (DLBCSOOPJ01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Java Sprachkonzept und erste Java-Programme
- Datentypen, Operatoren, Kontrollstrukturen und Methoden
- Objektorientierte Modellierung
- Klassen und Objekte
- Vererbung und Polymorphie
- Abstrakte Klassen und Schnittstellen
- Weiterführende Konzepte

Qualifikationsziele des Moduls

Grundlagen der objektorientierten Programmierung mit Java

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundkonzepte der objektorientieren 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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Grundlagen der objektorientierten Programmierung mit Java

Kurscode: DLBCSOOPJ01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 objektorientieren 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. Java Sprachkonzept und erste Java-Programme
   - 1.1 Übersetzungskonzept – Compiler und Interpreter
   - 1.2 Erstes Java-Programm – main()-Methode
   - 1.3 Erste Klassen und Objekte in Java
   - 1.4 Ein- und Ausgabe auf der Konsole
   - 1.5 Testen von Java-Programmen

2. Datentypen, Operatoren, Kontrollstrukturen und Methoden
   - Datentypen
   - Operatoren
   - Kontrollstrukturen
   - Parametrisierung von Methoden

3. Objektorientierte Modellierung
   - Objektorientierung im Software-Entwicklungsprozess
   - Von der Realität zum Modell

- Objektorientierte Prinzipien

4. Klassen und Objekte
   - Instanzvariable und Instanzmethoden
   - Objekt-Erzeugung und Konstruktoren
   - Die this-Referenz
   - Überladen von Methoden
   - Klassenvariable und Klassenmethoden

5. Vererbung und Polymorphie
   - Das Konzept der Vererbung
   - Die Klasse Object
   - Polymorphie und Überschreiben

6. Abstrakte Klassen und Schnittstellen
   - Optimierung von Vererbungshierarchien
   - Trennung von Spezifikation und Implementierung
   - Schnittstellen

7. Weiterführende Konzepte
   - Ausnahmebehandlung
   - Pakete und Klassenbibliotheken
   - Kompaktschreibweisen in der Java-Syntax

Literatur

Pflichtliteratur

Weiterführende Literatur

- Abts, D. (2024). Grundkurs JAVA: Von den Grundlagen bis zu Datenbank- und Netzanwendungen.
- Dörn, S. (2023). Java lernen in abgeschlossenen Lerneinheiten: Der Einstieg in die Programmierung mit vielen Beispielen. Springer Fachmedien Wiesbaden.
- Riesen, K. (2021). Java in 14 Wochen: Ein Lehrbuch für Studierende der Wirtschaftsinformatik. Springer Vieweg.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Mathematik: Lineare Algebra

Modulcode: DLBBIM

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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	Teilmodulprüfung
Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für weitere Module im Bereich Methoden	Alle Bachelor-Programme im Bereich Wirtschaft & Management

Mathematik: Lineare Algebra

Kurscode: DLBBIM01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
☑ Recorded Live Sessions	☑ Audio	☑ Online Tests
	☑ Folien	

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
	☑ Audio	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
☑ Recorded Live Sessions	☑ Audio	☑ Online Tests
	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
	☑ Audio	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Kollaboratives Arbeiten

Modulcode: DLBKA

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Karin Halbritter (Kollaboratives Arbeiten)

Kurse im Modul

- Kollaboratives Arbeiten (DLBKA01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: myStudium Fachpräsentation Studienformat: Duales myStudium Fachpräsentation Studienformat: Kombistudium Fachpräsentation Studienformat: Fernstudium Fachpräsentation	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Betriebswirtschaft & Management	Alle Bachelor-Programme im Bereich Wirtschaft

Kollaboratives Arbeiten

Kurscode: DLBKA01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Fachpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Fachpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Online Tests
- ☑ Prüfungsleitfaden

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Fachpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Fachpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Einführung in die Netzwerkforensik

Modulcode: DLBCSEINF_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum	DLBIBRVS01 oder DLBIBRVS01_E	BA	5	150 h

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

Modulverantwortliche(r)

Prof. Dr. Jörn-Marc Schmidt (Einführung in die Netzwerkforensik)

Kurse im Modul

- Einführung in die Netzwerkforensik (DLBCSEINF01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: myStudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung.	Alle Bachelor-Programme im Bereich IT & Technik.

Einführung in die Netzwerkforensik

Kurscode: DLBCSEINF01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Netzwerkspuren, 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, GeoIP- und WhoIs-Daten
    - 10.4 Zertifikat-Transparenz
    - 10.5 Korrelationsmethoden

Literatur

Pflichtliteratur

Weiterführende Literatur

- Cole, E., Krutz, R. L., & Conley, J. (2009). Network security bible. John Wiley & Sons.
- Kurose, J., & Ross, K. (2016). Computer networking: A top-down approach. Pearson Education.
- Stevens, F. (2014). TCP/IP illustrated (2. Auflage, Vol. 1—The protocols). Pearson.
- Tanenbaum, A., & Wetherall, D. (2013). Computer networks. Pearson Education.

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Requirements Engineering

Modulcode: IREN

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Tobias Brückmann (Requirements Engineering)

Kurse im Modul

- Requirements Engineering (IREN01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: myStudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Requirements Engineering

Kurscode: IREN01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Grundzüge des System-Pentestings

Modulcode: DLBCSESPB_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Stephan Spitz (Grundzüge des System-Pentestings)

Kurse im Modul

- Grundzüge des System-Pentestings (DLBCSESPB01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Grundzüge des System-Pentestings

Kurscode: DLBCSESPB01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

3. Semester

Interkulturelle und ethische Handlungskompetenzen

Modulcode: DLBIHK

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Jürgen-Matthias Seeler (Interkulturelle und ethische Handlungskompetenzen)

Kurse im Modul

- Interkulturelle und ethische Handlungskompetenzen (DLBIHK01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: myStudium Schriftliche Ausarbeitung: Fallstudie Studienformat: Fernstudium Schriftliche Ausarbeitung: Fallstudie Studienformat: Duales myStudium Schriftliche Ausarbeitung: Fallstudie Studienformat: Kombistudium Schriftliche Ausarbeitung: Fallstudie	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Methoden	Alle Bachelor-Programme im Bereich Wirtschaft

Interkulturelle und ethische Handlungskompetenzen

Kurscode: DLBIHK01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Hofstedes 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

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Online Tests
- ☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Einführung in das Internet of Things

Modulcode: DLBINGEIT

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Marian Benner-Wickner (Einführung in das Internet of Things)

Kurse im Modul

- Einführung in das Internet of Things (DLBINGEIT01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Klausur oder Fachpräsentation, 90 Minuten Studienformat: Kombistudium Klausur oder Fachpräsentation, 90 Minuten Studienformat: myStudium Klausur oder Fachpräsentation, 90 Minuten Studienformat: Fernstudium Klausur oder Fachpräsentation, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Grundlagen des Internet of Things
- Gesellschaftliche und wirtschaftliche Bedeutung
- Kommunikationsstandards und -technologien
- Datenspeicherung und -verarbeitung
- Design und Entwicklung
- Anwendungsbereiche

Qualifikationsziele des Moduls

Einführung in das Internet of Things

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.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Einführung in das Internet of Things

Kurscode: DLBINGEIT01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 ihnen 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 vernetzer 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

Literatur

Pflichtliteratur

Weiterführende Literatur

- Andelfinger, V. P., & Hänisch, T. (Hrsg.). (2015). Internet der Dinge. Technik, Trends und Geschäftsmodelle. Springer.
- Buyya, R., & Vahid Dastjerdi, A. (Hrsg.). (2016). Internet of things. Principles and paradigms. Morgan Kaufmann.
- Christoph, E., & Sprenger, F. (Hrsg.). (2015). Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt. transcript.
- Fleisch, E. (Hrsg.). (2005). Internet der dinge. Ubiquitous Computing und RFID in der Praxis. Springer.
- Gilchrist, A. (2016). Industry 4.0. The industrial internet of things. Apress.
- Herrero, R. (2022). Network and Transport Layers. In Fundamentals of IoT Communication Technologies. Textbooks in Telecommunication Engineering.
- Kaufmann, T. (2015). Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge. Der Weg vom Anspruch in die Wirklichkeit. Springer.
- Schallmo, D. R. A., et al. (2021). Digitale Transformation von Geschäftsmodellen. Schwerpunkt Business Model Innovation. Springer Gabler.
- Stumpf, E. (2020). Industrie 4.0 in der Luft- und Raumfahrt. In Frenz, W. (Hrsg.), Handbuch Industrie 4.0: Recht, Technik, Gesellschaft (S. 759–776). Springer.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Fachpräsentation, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	☑ Prüfungsleitfaden
	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Fachpräsentation, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Fachpräsentation, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Fachpräsentation, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Algorithmen, Datenstrukturen und Programmiersprachen

Modulcode: DLBIADPS-01

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum	DLBDSIPWP01_D oder DLBCSOOPJ01_D oder DLBMINPAPCC01 oder DLBROEPRS01_D	BA	5	150 h

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

Modulverantwortliche(r)

Prof. Dr. Jörn-Marc Schmidt (Algorithmen, Datenstrukturen und Programmiersprachen)

Kurse im Modul

- Algorithmen, Datenstrukturen und Programmiersprachen (DLBIADPS01-01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Advanced Workbook Studienformat: myStudium Advanced Workbook Studienformat: Fernstudium Advanced Workbook	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Datenstrukturen
- Algorithmenentwurf
- Grundlegende Algorithmen
- Strukturierte Daten repräsentieren
- Programmierparadigmen und Grundbegriffe von Programmiersprachen
- Überblick über wichtige Programmiersprachen

Qualifikationsziele des Moduls

Algorithmen, Datenstrukturen und Programmiersprachen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Datenstrukturen und Algorithmen zu erklären, beschreiben und anwenden.
- grundlegende Konstrukte der Aussagenlogik in der Programmierung anzuwenden.
- die Struktur von Rechnerhardware zu beschreiben.
- Dokumentenverarbeitungsbibliotheken anzuwenden.
- Programmierparadigmen vergleichen und die Programmiersprachen einzuordnen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Algorithmen, Datenstrukturen und Programmiersprachen

Kurscode: DLBIADPS01-01

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
BA	Deutsch		5	DLBDSIPWP01_D oder DLBCSOOPJ01_D oder DLBMINPAPCC01 oder DLBROEPRS01_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 und Algorithmen zu erklären, beschreiben und anwenden.
- grundlegende Konstrukte der Aussagenlogik in der Programmierung anzuwenden.
- die Struktur von Rechnerhardware zu beschreiben.
- Dokumentenverarbeitungsbibliotheken anzuwenden.
- Programmierparadigmen vergleichen und die Programmiersprachen einzuordnen.

Kursinhalt

1. Grundbegriffe der Datenverarbeitung
   - 1.1 Algorithmen, Datenstrukturen und Programmiersprachen als Grundlagen der
   - 1.2 Programmierung
   - 1.3 Detaillierung und Abstraktion
   - 1.4 Kontrollstrukturen
   - 1.5 Datentypen
   - 1.6 Grundlegenden Datenstrukturen (Liste, Kette, Baum)

2. Datenstrukturen
   - 2.1 Weiterführende Datenstrukturen: Queue, Heap, Stack und Graph
   - 2.2 Abstrakte Datentypen, Objekte und Klassen

- 2.3 Polymorphismus

3. Algorithmendesign
   - 3.1 Iteration, Rekursion und Induktion
   - 3.2 Methoden des Algorithmenendesigns
   - 3.3 Korrektheit und Verifikation von Algorithmen
   - 3.4 Effizienz (Komplexität) von Algorithmen

4. Grundlegende Algorithmen
   - 4.1 Traversierung und Linearisierung von Bäumen
   - 4.2 Suchalgorithmen
   - 4.3 Sortieralgorithmen
   - 4.4 Suchen in Zeichenketten
   - 4.5 Hash-Algorithmen
   - 4.6 Mustererkennung

5. Darstellung strukturierter Daten
   - 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 Alternative Dokumentdarstellungen

6. Programme messen
   - 6.1 Typinferenz und interaktive IDE-Unterstützung
   - 6.2 Zyklomatische Komplexität
   - 6.3 Aufbereitung der Codedokumentation
   - 6.4 Compiler-Optimierung
   - 6.5 Codeabdeckung
   - 6.6 Unit- und Integrationstests
   - 6.7 Heap-Analyse

7. Programmiersprachen
   - 7.1 Programmierparadigmen
   - 7.2 Ausführung von Programmen
   - 7.3 Typen von Programmiersprachen
   - 7.4 Syntax, Semantik und Pragmatik
   - 7.5 Variablen und Typsysteme

8. Wichtige Programmiersprachen

8.1 Assembler und Webassembly
8.2 C und C++
8.3 Java und C#
8.4 Haskell und Lisp
8.5 JavaScript und seine Verwandten
8.6 Andere imperative 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 Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Online Tests
- ☑ Prüfungsleitfaden

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Online Tests
- ☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Theoretische Informatik und Mathematische Logik

Modulcode: DLBITIML

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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 (Theoretische Informatik und Mathematische Logik)

Kurse im Modul

- Theoretische Informatik und Mathematische Logik (DLBITIML01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Theoretische Informatik und Mathematische Logik

Kurscode: DLBITIML01

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

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 Zustandsübergangsdiagrammen, 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 ndirekter 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

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Dewdney, A.K. (1995): Der Turing Omnibus. Eine Reise durch die Informatik mit 66 Stationen. Springer, Berlin/Heidelberg/New York. ▪ Erk, K./Priese, L. (2008): Theoretische Informatik. 3. Auflage. Springer eXamen.press, Berlin/ Heidelberg. ▪ Priese, L./Wimmerl, H. (2008): Petri-Netze. 2. Auflage. Springer eXamen.press, Berlin/ Heidelberg. ▪ Schöning, U. (2000): Logik für Informatiker. 5. Auflage. Spektrum Verlag, Heidelberg/ Berlin. ▪ Schöning, U. (2008): Ideen der Informatik. Grundlegende Modelle und Konzepte der Theoretischen Informatik, 3. Auflage. Oldenbourg, München.

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
☑ Recorded Live Sessions	☑ Folien	☑ Online Tests

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
☑ Recorded Live Sessions	☑ Folien	☑ Online Tests

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
☑ Recorded Live Sessions	☑ Folien	☑ Online Tests

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
☑ Recorded Live Sessions	☑ Folien	☑ Online Tests

IT-Projektmanagement

Modulcode: IPMG-01

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Tobias Brückmann (IT-Projektmanagement)

Kurse im Modul

- IT-Projektmanagement (IPMG01-01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Begriffe und Grundlagen im IT-Projektmanagement
- Planungstechniken im Großen und Kleinen
- Techniken zu Priorisierung, Aufwandschätzung, Projektcontrolling
- Techniken zu Stakeholder-, Kommunikations- und Risikomanagement
- Organisation und Struktur von IT-Projekten
- PITPM - Pragmatisches IT- Projektmanagement

Qualifikationsziele des Moduls

IT-Projektmanagement

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundprinzipien und Aufgaben von IT-Projektmanagement zu erläutern und voneinanderabzugrenzen.
- Techniken zur Planung und zur operativen Steuerung von IT-Projekten zu erläutern undvoneinander abzugrenzen.
- ausgewählte Techniken und Methoden zum Stakeholder-, Kommunikations- und Risikomanagementzu 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.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

IT-Projektmanagement

Kurscode: IPMG01-01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 voneinanderabzugrenzen.
- Techniken zur Planung und zur operativen Steuerung von IT-Projekten zu erläutern undvoneinander abzugrenzen.
- ausgewählte Techniken und Methoden zum Stakeholder-, Kommunikations- und Risikomanagementzu 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.
- Spitczok 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 GovernancePublishing.

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

DevSecOps und gängige Software-Schwachstellen

Modulcode: DLBCSEDCSW_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum	DLBCSESPB01_D oder DLBCSESPB01_E	BA	5	150 h

Semester	Dauer	Regulär angeboten im	Kurs- und Prüfungssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	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	Teilmodulprüfung
Studienformat: Fernstudium Schriftliche Ausarbeitung: Hausarbeit Studienformat: Duales myStudium Schriftliche Ausarbeitung: Hausarbeit Studienformat: myStudium Schriftliche Ausarbeitung: Hausarbeit	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

DevSecOps und gängige Software-Schwachstellen

Kurscode: DLBCSEDCSW01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Hausarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Hausarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Hausarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

4. Semester

IT-Servicemanagement

Modulcode: DLBCSITSM1-01_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. André Köhler (IT-Servicemanagement)

Kurse im Modul

- IT-Servicemanagement (DLBCSITSM01-01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Kombistudium Klausur Studienformat: Duales myStudium Klausur Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: myStudium Klausur	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Grundlagen und Begriffe des IT-Servicemanagements
- ITIL 4 – Grundlagen und vier Dimensionen
- ITIL 4 – Das Service Value System
- ITIL 4 – Prinzipien
- ITIL 4 – Praktiken
- Informationssicherheitsmanagement mit dem IT-Grundschutz des BSI

Qualifikationsziele des Moduls

IT-Servicemanagement

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme aus dem Bereich IT & Technik

IT-Servicemanagement

Kurscode: DLBCSITSM01-01_D

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

Beschreibung des Kurses

IT-Servicemanagement 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-Servicemanagement (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-Servicemanagements zu benennen.
- die Motivation und den Aufbau der IT Infrastructure Library (ITIL) zu beschreiben, die Hauptelemente zu bestimmen und konkrete Aktivitäten im Service Livecycle 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 des IT-Servicemanagements
   - 1.1 IT-Services
   - 1.2 IT-Servicemanagement
   - 1.3 ITSM-Frameworks
2. ITIL 4 – Grundlagen und vier Dimensionen
   - 2.1 Stakeholder, Services und Servicemanagement
   - 2.2 Wertbeitrag der IT
   - 2.3 Vier-Dimensionen-Modell
3. ITIL 4 – Service Value System
   - 3.1 Grundlagen und Überblick
   - 3.2 Inputs, Ergebnisse und Governance

3.3 Die Service-Wertschöpfungskette
3.4 Kontinuierliche Verbesserung

4. ITIL 4 – Prinzipien
   4.1 Übersicht
   4.2 Wertorientierung
   4.3 Iteratives Verfahren und Feedback
   4.4 Zusammenarbeit und Transparenz etablieren
   4.5 Optimieren und Automatisieren

5. ITIL 4 – Praktiken
   5.1 Übersicht
   5.2 Allgemeine Managementpraktiken
   5.3 Praktiken des Servicemanagements
   5.4 Technische Praktiken

6. Informationssicherheitsmanagement mit dem IT-Grundschutz des BSI
   6.1 Struktur und Elemente des IT-Grundschutzes des BSI
   6.2 Informationssicherheitsprozess

Literatur

Pflichtliteratur

Weiterführende Literatur

- Axelos Limited. (2020). ITIL 4: Direct, plan, and improve. The Stationery Office, Chapters 3—10.
- Beims, M. (2021). IT-Service Management in der Praxis mit ITIL® Zusammenarbeit systematisieren und relevante Ergebnisse erzielen. Hanser.
- Ebel, N. (2021). Basiswissen ITIL 4 [electronic resource]: Grundlagen und Know-how für das IT Service Management und die ITIL-4-Foundation-Prüfung (1. Auflage). Dpunkt.verlag.
- Kersten, H. (2020). IT-Sicherheitsmanagement nach der neuen ISO 27001 ISMS, Risiken, Kennziffern, Controls. Springer Vieweg.
- Limited, A. (2020). ITIL 4 [electronic resource]: Create, Deliver and Support. TSO.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessi-ons/Learning Sprint	☑ Video	☑ Online Tests
	☑ Folien	
☑ Recorded Live Sessions		

Kryptografische Verfahren

Modulcode: DLBISIC2-01

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Ralf Kneuper (Kryptografische Verfahren)

Kurse im Modul

- Kryptografische Verfahren (DLBISIC02-01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Schriftliche Ausarbeitung: Fallstudie Studienformat: Duales myStudium Schriftliche Ausarbeitung: Fallstudie Studienformat: Kombistudium Schriftliche Ausarbeitung: Fallstudie Studienformat: myStudium Schriftliche Ausarbeitung: Fallstudie	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Schutzziele, Schwachstellen und Bedrohungen
- Kryptologische Grundlagen und kryptografische Bausteine
- Kryptografische Grundanwendungen
- Authentifikation
- Sicherung von Einzelrechnern
- Sicherheit in Kommunikationsnetzen
- Sicherheit im E-Commerce
- Sichere Softwareentwicklung

Qualifikationsziele des Moduls

Kryptografische Verfahren

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.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme im Bereich IT & Technik

Kryptografische Verfahren

Kurscode: DLBISIC02-01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 ▪ Beutelspacher, A., Schwenk, J., & Wolfenstetter, K. (2022). Moderne Verfahren der Kryptographie. Springer Spektrum. ▪ Eckert, C. (2018). IT-Sicherheit: Konzepte – Verfahren – Protokolle (10. Aufl.). Oldenbourg Wissenschaftsverlag. ▪ Ertel, W. (2019). Angewandte Kryptographie (6. Aufl.). Carl Hanser. ▪ Glemser, T. (2022). OWASP Top 10. Datenschutz und Datensicherheit, 46(8), 695–698.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Folien	

IT-Recht

Modulcode: DLBIITR-01

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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)

Andreas Gronemann (IT-Recht)

Kurse im Modul

- IT-Recht (DLBIITR01-01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Duales Studium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- IT-Recht und seine Einbettung in das Rechtssystem
- Vertragstypen
- Softwarelizenzmodelle
- Schutz- und Informationsrechte
- Internetrecht und Telekommunikationsrecht
- Datenschutz

Qualifikationsziele des Moduls

IT-Recht

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wesentlichen nationalen und internationalen Rechtsgrundlagen und Rahmenbedingungen des IT-Rechtes zu benennen.
- in Anwendungsfällen die geeignete Vertragsform oder das geeignete Lizenzmodell
- die verschiedenen Schutz- und Informationsrechte zu erläutern.
- die rechtlichen Grundlagen zum Datenschutzrecht auf einfache Anwendungsfälle anzuwenden.
- 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.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für weitere Module im Bereich Recht	Alle Bachelor-Programme im Bereich Management

IT-Recht

Kurscode: DLBIITR01-01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 juristischen Knowhow erforderlich wird.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wesentlichen nationalen und internationalen Rechtsgrundlagen und Rahmenbedingungen des IT-Rechtes zu benennen.
- in Anwendungsfällen die geeignete Vertragsform oder das geeignete Lizenzmodell
- die verschiedenen Schutz- und Informationsrechte zu erläutern.
- die rechtlichen Grundlagen zum Datenschutzrecht auf einfache Anwendungsfälle anzuwenden.
- 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
   - 1.7 Grundlagen der Vertragsschließung und -gestaltung
2. Typische Vertragstypen in der IT und Onlineverträge

- 2.1 Hardware-Verträge
- 2.2 Softwareüberlassung
- 2.3 Projektverträge
- 2.4 Besonderheiten bei agiler Vorgehensweise
- 2.5 Beratungs-, Schulungs- und Wartungsverträge
- 2.6 Cloud Computing, Outsourcing und Hosting
- 2.7 Elektronische Vertragsschließung
- 2.8 Elektronischer Geschäftsverkehr und Online-Marktplätze

3. Softwarelizenzmodelle
   - 3.1 Lizenzen und Softwareüberlassung
   - 3.2 IT-spezifische 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 Kennzeichenrecht
   - 4.2 Urheberrecht
   - 4.3 Schutzfähigkeit von Software
   - 4.4 Schutzfähigkeit von Datenbanken bzw. Datenbankherstellern
   - 4.5 Abmahnungen
   - 4.6 Informationsfreiheitsgesetz

5. Internet- und Telekommunikationsrecht
   - 5.1 Telekommunikationsgesetz
   - 5.2 Medienstaatsvertrag
   - 5.3 Informationspflicht nach dem Digitale-Dienste-Gesetz
   - 5.4 Verantwortung für Inhalte im Internet
   - 5.5 Domainrecht
   - 5.6 Elektronische Signaturen

6. Datenschutz, IT-Sicherheit und Produkthaftung
   - 6.1 Grundlagen des Datenschutzes
   - 6.2 DSGVO, BDSG und TDDDG
   - 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. ▪ Hoeren, T. (2017). IT-Recht. Skriptum. Abgerufen von https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien ▪ Sodtalbers, A., Volmann, A. & Heise, A. (2010). IT-Recht. W3L Verlag. ▪ Voigt, P. & von dem Bussche, A. (2018). EU-Datenschutz-Grundverordnung (DSGVO). Praktikerhandbuch. Springer. ▪ Zahrnt, C. (2014). IT-Projektverträge. Rechtlich richtig vorgehen. CreateSpace Independent Publishing Platform.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Duales Studium

Studienform	**Kursart**
Duales Studium	Integrierte Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium/ synchrone virtuelle Lehre**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
129,75 h	13,5 h	6,75 h	0 h	0 h	150 h

Lehrmethoden
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 Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Host- und Softwareforensik

Modulcode: DLBCSEHSF_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum	DLBCSESPB01_D oder DLBCSESPB01_E	BA	5	150 h

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

Modulverantwortliche(r)

Prof. Dr. Petra Beenken (Host- und Softwareforensik)

Kurse im Modul

- Host- und Softwareforensik (DLBCSEHSF01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung.	Alle Bachelor-Programme im Bereich IT & Technik.

Host- und Softwareforensik

Kurscode: DLBCSEHSF01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Computerforensik
   - 1.1 Grundlagen der Untersuchung: Strafrecht oder Unternehmensrichtlinien
   - 1.2 Richtlinien, rechtliche Rahmenbedingungen und Standards
   - 1.3 Sachverständige
2. Digitale Beweise
   - 2.1 Arten von Beweisen
   - 2.2 Sicherung und Chain of Custody

- 2.3 Identifikation
- 2.4 Bewertung
- 2.5 Präsentation

3. Zusammenstellung der Beweise aus den Systemen
   - 3.1 Software-Tools und Hardware-Unterstützung
   - 3.2 Kryptografische Methoden zur Sicherstellung der Integrität und der Chain of Custody
   - 3.3 Schritte bei der Durchsuchung eines Tatorts
   - 3.4 Cloud Computing und mobile Endgeräte
   - 3.5 Mobilgeräte
   - 3.6 Festplatten und SSD

4. Systemforensik
   - 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. Sandboxing von Schadsoftware
   - 5.1 Arten von Schadsoftware
   - 5.2 Kommerzielle und Open-Source-Tools
   - 5.3 Betrachtungen im Gastsystem
   - 5.4 Ausführung von inaktiver, langsamer oder verzögerter Malware
   - 5.5 Interpretation von Berichten der Sandbox

6. Prinzipien des Reverse Engineering
   - 6.1 Reinraumumgebung
   - 6.2 Prinzipien der Disassemblierung
   - 6.3 Maschinencode
   - 6.4 Dekompilierung

7. Auswertung
   - 7.1 Zusammenhänge herstellen
   - 7.2 Ursachenanalyse
   - 7.3 Zuordnung zu MITRE ATT&CK® Techniken, Taktiken und Verfahren
   - 7.4 Vermeidung vorschneller Schlüsse

8. Präsentation
   - 8.1 Verfassen des Berichts

8.2 Zusammenarbeit mit den Strafverfolgungsbehörden
8.3 Vorbereitung für die Präsentation vor Gericht
8.4 Vorbereitung der Präsentation für Führungskräfte

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 Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Artificial Intelligence

Modulcode: DLBDSEAIS1_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Kristina Schaaff (Artificial Intelligence)

Kurse im Modul

- Artificial Intelligence (DLBDSEAIS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten Studienformat: Kombistudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Data Science & Artificial Intelligence	Alle Bachelor Programme im Bereich IT & Technik

Artificial Intelligence

Kurscode: DLBDSEAIS01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

- Brett, J. M., Friedman, R., & Behfar, K. (2009). How to manage your negotiating team. Harvard Business Review, 87(9), 105–109.
- Buchanan, B. G. (2005). A (very) brief history of artificial intelligence. AI Magazine, 26(4), 53–60.
- Cole, E., Krutz, R. L., & Conley, J. (2009). Network security bible. John Wiley & Sons.
- Kurose, J., & Ross, K. (2016). Computer networking: A top-down approach. Pearson Education.
- Mikolov, T., Chen, K., Corrado, G., & Dean, J. (2013). Efficient estimation of word representations in vector space. ArXiv.
- Russell, S. & Norvig, P. (2023). Künstliche Intelligenz. (4.Auflage). Pearson Deutschland.
- Stevens, F. (2014). TCP/IP illustrated (2. Aufl., Vol. 1—The protocols). Pearson.
- Tanenbaum, A., & Wetherall, D. (2013). Computer networks. Pearson Education.

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Standards der Informationssicherheit

Modulcode: DLBCSEISS_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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)

Dilan Özdemir-Kaluk (Standards der Informationssicherheit)

Kurse im Modul

- Standards der Informationssicherheit (DLBCSEISS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Schriftliche Ausarbeitung: Fallstudie Studienformat: myStudium Schriftliche Ausarbeitung: Hausarbeit Studienformat: Fernstudium Schriftliche Ausarbeitung: Fallstudie	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Bachelor-Programme aus dem Bereich IT & Technik

Standards der Informationssicherheit

Kurscode: DLBCSEISS01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Normen und regulatorische Rahmenbedingungen
   - 1.3 Sicherheitsnormen: ISO/IEC 27000-Familie und BSI-Normen
   - 1.4 Managementsystem für Informationssicherheit (ISMS)
2. Initiierung eines Managementsystems für Informationssicherheit
   - 2.1 Ersteinrichtung des ISMS
   - 2.2 Analyse des Unternehmens
   - 2.3 Analyse des bestehenden ISMS und Bestimmung des Reifegrads
   - 2.4 Definition des ISMS-Anwendungsbereichs und der Sicherheitspolitiken
3. Implementierung des Managementsystem für Informationssicherheit
   - 3.1 Risikobeurteilung
   - 3.2 Erklärung zur Anwendbarkeit (SoA)
   - 3.3 Definition der Unternehmensstruktur für Informationssicherheit
   - 3.4 Dokumentenmanagement und Kommunikationsplan

3.5 Definition von Maßnahmen und Verfahren

4. Controlling des Managementsystems für Informationssicherheit
   - 4.1 Überwachung, Messung, Analyse und Auswertung
   - 4.2 Internes Audit
   - 4.3 Management Review

5. Verbesserung des Managementsystems für Informationssicherheit
   - 5.1 Betrachtung von Herausforderungen und Abweichungen
   - 5.2 Fortlaufende Verbesserung
   - 5.3 Pläne für Korrektur- und Präventivmaßnahmen

6. Maßnahmen des Managementsystems für Informationssicherheit
   - 6.1 Allgemeine Struktur von Maßnahmen
   - 6.2 Maßnahmen der ISO/IEC 27001 - Anhang A
   - 6.3 Maßnahmenmanagement
   - 6.4 Bewertung der Wirksamkeit von Maßnahmen

Literatur

Pflichtliteratur

Weiterführende Literatur

- Brotherston, L. & Berlin, A. (2017). Defensive security handbook: Best practices for securing infrastructure. O'Reilly Media.
- Campbell, T. (2016). Practical information security management: A complete guide to planning and implementation. Apress.
- Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2015). Foundations of information security based on ISO27001 and ISO27002 (3. Aufl.). Van Haren Publishing.
- Viegas, V. & Kuyucu, O. (2022). IT Security Controls: A guide to corporate standards and frameworks. Apress.

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Hausarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

5. Semester

Seminar: Aktuelle Themen in Computer Science

Modulcode: DLBCSSCTCS_D

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

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

Modulverantwortliche(r)

Alexander Christopher Bock (Seminar: Aktuelle Themen in Computer Science)

Kurse im Modul

- Seminar: Aktuelle Themen in Computer Science (DLBCSSCTCS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: myStudium Schriftliche Ausarbeitung: Seminararbeit Studienformat: Fernstudium Schriftliche Ausarbeitung: Seminararbeit Studienformat: Duales myStudium Schriftliche Ausarbeitung: Seminararbeit	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung.	Alle Bachelor-Programme im Bereich IT & Technik.

Seminar: Aktuelle Themen in Computer Science

Kurscode: DLBCSSCTCS01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 myStudium

Studienform	**Kursart**
myStudium	Seminar

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Seminararbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Seminar

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Seminararbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Seminar

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Seminararbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Advanced Data Analysis

Modulcode: DLBDSEDA1_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Thomas Zöller (Advanced Data Analysis)

Kurse im Modul

- Advanced Data Analysis (DLBDSEDA01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Data Science & Artificial Intelligence	Alle Bachelor-Programme im Bereich IT & Technik

Advanced Data Analysis

Kurscode: DLBDSEDA01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Projekt: Datenanalyse

Modulcode: DLBDSEDA2_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Frank Passing (Projekt: Datenanalyse)

Kurse im Modul

- Projekt: Datenanalyse (DLBDSEDA02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: myStudium Portfolio Studienformat: Duales myStudium Portfolio Studienformat: Fernstudium Portfolio	

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: Datenanalyse

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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Data Science & Artificial Intelligence	Alle Bachelor-Programme im Bereich IT & Technik

Projekt: Datenanalyse

Kurscode: DLBDSEDA02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Speziell im dualen Fernstudium:
Im dualen Fernstudium ist der Theorie-Praxis-Transfer anhand eines realen Projekts, das im Praxisbetrieb umgesetzt werden soll, zu leisten. Im Rahmen des Praxisprojektes bearbeiten die Studierenden eine praxisrelevante Fragestellung ihres Praxisbetriebs unter Betreuung einer:s Lehrenden. Eine Betreuung seitens Praxispartner kann auf Wunsch erfolgen.

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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

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 myStudium

Studienform	Kursart
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Portfolio

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Portfolio

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	30 h	0 h	120 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Portfolio

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Cloud Computing

Modulcode: DLBDSCC_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Tianxiang Lu (Cloud Computing)

Kurse im Modul

- Cloud Computing (DLBDSCC01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten Studienformat: Duales myStudium Klausur, 90 Minuten Studienformat: myStudium Klausur, 90 Minuten	

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist Grundlage für alle weiteren Module aus dem Bereich Data Science & Artificial Intelligence	Alle Bachelor-Programme im Bereich IT & Technik

Cloud Computing

Kurscode: DLBDSCC01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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.
- Kratzke, N. (2022). Cloud-Native Computing – Software Engineering von Diensten und Applikationen für die Cloud, Carl Hanser Verlag.
- Mahmood, Z.,Puttini, R.& Erl, T. (2013). Cloud computing: Concepts, technology & architecture. Prentice Hall, Boston, MA.
- Rafaels, R. (2018). Cloud computing (2nd ed.). 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

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Repetitorium
☑ Recorded Live Sessions	☑ Audio	☑ Prüfungsleitfaden
	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

IT-Sicherheitsberatung

Modulcode: DLBCSEEISC_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Rainer Lukas (Technische und betriebliche IT-Sicherheitskonzeptionen) / Nils Kannengießer (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 "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "myStudium": Klausur, 90 Minuten Projekt: Einsatz und Konfiguration von SIEM-Systemen • Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Duales myStudium": 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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Technische und betriebliche IT-Sicherheitskonzeptionen

Kurscode: DLBCSEEISC01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Datenfluss, Interdependenzen und Interrelationen
   - 1.3 Überprüfung und Erkennen von Schwachstellen
   - 1.4 Unterstützende Tools und Techniken

2. Schutzprofile
   - 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 und Sensoren
   - 3.3 Analytik
   - 3.4 Indicators of Compromise - Indikatoren für Kompromittierungen

4. Netzwerküberwachung
   - 4.1 Advanced Threat Protection (ATP)
   - 4.2 Technologie drahtloser Sensornetzwerke
   - 4.3 Austausch von Bedrohungsinformationen

5. Sicherheitsinformationen und Ereignismanagement (SIEM)
   - 5.1 Technische und betriebliche Datenquellen
   - 5.2 Datenfusion
   - 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-Sicherheitsmetriken
   - 6.2 Bewertung der IT-Sicherheit

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Bundesamt für Sicherheit in der Informationstechnik. (2023). BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen. ▪ Eckert, C. (2018). IT-Sicherheit: Konzepte – Verfahren – Protokolle (10. Aufl.). De Gruyter Oldenbourg. ▪ Kappes, M. (2022). Netzwerk- und Datensicherheit: Eine praktische Einführung. Springer Fachmedien. ▪ Kloep, P., & Weigel, K. (2023). Sichere Windows-Infrastrukturen: Das Handbuch für Administratoren. Rheinwerk Computing. ▪ Wendzel, S. (2018). IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung. Springer Fachmedien.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Audio
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Projekt: Einsatz und Konfiguration von SIEM-Systemen

Kurscode: DLBCSEEISC02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Speziell im dualen Fernstudium: Im dualen Fernstudium ist der Theorie-Praxis-Transfer anhand eines realen Projekts, das im Praxisbetrieb umgesetzt werden soll, zu leisten. Im Rahmen des Praxisprojektes bearbeiten die Studierenden eine praxisrelevante Fragestellung ihres Praxisbetriebs unter Betreuung einer:s Lehrenden. Eine Betreuung seitens Praxispartner kann auf Wunsch erfolgen.

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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

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
- 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 myStudium

Studienform	Kursart
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	30 h	0 h	120 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Social Engineering

Modulcode: DLBCSEESE_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Nils Kannengießer (Social Engineering und Insider Threats) / Rami Alkubaty (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 "myStudium": Schriftliche Ausarbeitung: Fallstudie • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Fallstudie • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Fallstudie Projekt: Social Engineering • Studienformat "Duales myStudium": Projektpräsentation • Studienformat "Fernstudium": Projektpräsentation • Studienformat "myStudium": 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 Internetdienstanbietern zusammenzuarbeiten.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Social Engineering und Insider Threats

Kurscode: DLBCSEESE01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 so genannten "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 Quidproquo, Köder (Baiting), Medienköder (Media Dropping)
   - 1.3 Scareware, Betrugsmasche CEO-Fraud (CEO-Betrug)
   - 1.4 Pretexting, Tailgating

2. Rechtliche Aspekte des Social Engineering
   - 2.1 Compliance, Verhaltenskodex
   - 2.2 Identitätsdiebstahl
   - 2.3 Datenschutz

3. Erkennung von Insider-Bedrohungen
   - 3.1 Data-Mining-Techniken
   - 3.2 Anwendung von Methoden des Machine Learning
   - 3.3 Umfassendes Framework für die Erkennung von und Reaktion auf Insider-Bedrohungen
   - 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 und internationale Zusammenarbeit sowie 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) sowie 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 myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Projekt: Social Engineering

Kurscode: DLBCSEESE02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Speziell im dualen Fernstudium: Im dualen Fernstudium ist der Theorie-Praxis-Transfer anhand eines realen Projekts, das im Praxisbetrieb umgesetzt werden soll, zu leisten. Im Rahmen des Praxisprojektes bearbeiten die Studierenden eine praxisrelevante Fragestellung ihres Praxisbetriebs unter Betreuung einer:s Lehrenden. Eine Betreuung seitens Praxispartner kann auf Wunsch erfolgen.

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 Internetdienstanbietern zusammenzuarbeiten.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

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 Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Projektpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	30 h	0 h	120 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Projektpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat myStudium

Studienform	Kursart
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Projektpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Host Forensics

Module Code: DLBCSEEHF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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

Mohammad Reza Rostami (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 • Study Format "myStudies": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes Seminar: Sandbox Interpretation • Study Format "myStudies": Written Assessment: Research Essay • Study Format "Duales myStudium": Written Assessment: Research Essay • 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	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	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 Understanding Malware: Components, Types, and Analysis
   - 1.2 Forensics
   - 1.3 Root Cause Analysis
   - 1.4 The MITRE Attack Framework
   - 1.5 Best Practices for Malware Prevention and Mitigation
2. Analysis Lab Setup
   - 2.1 Building a Secure Malware Analysis Lab
   - 2.2 Stealth
   - 2.3 Isolation
   - 2.4 Honeypots
3. Tools of the Trade
   - 3.1 Virtual Machines
   - 3.2 Debugger
   - 3.3 Anti Debugging Mechanism
   - 3.4 Disassembler

4. Malware Classification
   - 4.1 Malware Triage and Classification
   - 4.2 Structure of a Virus
   - 4.3 Antivirus
   - 4.4 VirusTotal
   - 4.5 Yara
   - 4.6 AI-assisted Malware Analysis

5. Sandboxes
   - 5.1 Different Sandbox Concepts and Their Purposes
   - 5.2 Levels of Interaction
   - 5.3 Instrumentation
   - 5.4 Online Sandboxing Services
   - 5.5 Sandbox Detection and Evasion

6. Reversing
   - 6.1 Understanding Malware Analysis and Its Impact
   - 6.2 Unpacking, Decrypting, and De-Obfuscation
   - 6.3 Debugging Techniques
   - 6.4 Control Flow Analysis
   - 6.5 Library and System Calls

7. Digging Deeper
   - 7.1 Threat Intelligence Integration
   - 7.2 Analysis of JavaScript Code
   - 7.3 Memory Forensics
   - 7.4 Understanding and Debugging Rootkits

Literature

Compulsory Reading

Further Reading

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

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ 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 myStudies

Study Format	Course Type
myStudies	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

DevSecOps

Modulcode: DLBCSEEDSO-01_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		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) / Prof. Dr. Jörn-Marc Schmidt (Projekt: Agiles DevSecOps-Software-Engineering)

Kurse im Modul

- Techniken und Methoden der agilen Softwareentwicklung (DLBWIWTMAS01)
- Projekt: Agiles DevSecOps-Software-Engineering (DLBCSEEDSO01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Techniken und Methoden der agilen Softwareentwicklung • Studienformat "Kombistudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "myStudium": Klausur, 90 Minuten • Studienformat "Duales myStudium": Klausur, 90 Minuten Projekt: Agiles DevSecOps-Software-Engineering • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • 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
- Agile Softwareentwicklung mit Scrum
- Agiles Portfolio- und Projektmanagement
- Requirements Engineering und agiles Architekturmanagement
- Agiles Testen
- Continuous Delivery

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,

- den Ansatz der agilen Softwareentwicklung zu charakterisieren und gegenüber der klassischen Softwareentwicklung abzugrenzen.
- den allgemeinen Aufbau und Ablauf eines Scrum-Projekts zu beschreiben.
- agile Techniken zur Durchführung der Kernaktivitäten des Software-Engineering zu erläutern und diese anzuwenden.
- die Methoden und Werkzeuge des Continuous-Delivery-Ansatzes zu erklären und die Relevanz des Ansatzes im Unternehmenskontext zu beurteilen.

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	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Techniken und Methoden der agilen Softwareentwicklung

Kurscode: DLBWIWTMAS01

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

Beschreibung des Kurses

Der Kurs vermittelt den Studierenden einen umfassenden Einblick in die agile Softwareentwicklung. Hierbei werden sowohl die grundlegenden agilen Prinzipien dargestellt als auch deren Anwendung im Kontext von kleinen und großen Softwareentwicklungsprojekten. Anhand praktischer Beispiele lernen die Studierenden agile Techniken zur Durchführung der Kernaktivitäten im Software-Engineering kennen. Als besonderer Schwerpunkt wird dabei auch auf den Ansatz des Continuous Delivery eingegangen und dessen Methoden und Werkzeuge vorgestellt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Ansatz der agilen Softwareentwicklung zu charakterisieren und gegenüber der klassischen Softwareentwicklung abzugrenzen.
- den allgemeinen Aufbau und Ablauf eines Scrum-Projekts zu beschreiben.
- agile Techniken zur Durchführung der Kernaktivitäten des Software-Engineering zu erläutern und diese anzuwenden.
- die Methoden und Werkzeuge des Continuous-Delivery-Ansatzes zu erklären und die Relevanz des Ansatzes im Unternehmenskontext zu beurteilen.

Kursinhalt

1. Merkmale und Prinzipien von Agilität
   - 1.1 Merkmale und Herausforderungen von Softwareprojekten
   - 1.2 Klassifikationen von Unsicherheit
   - 1.3 Gegenüberstellung von agiler und klassischer Softwareentwicklung
   - 1.4 Prinzipien der Agilität
2. Agile Softwareentwicklung mit Scrum
   - 2.1 Grundlagen und allgemeiner Aufbau von Scrum
   - 2.2 Zentrales Managementartefakt: Product Backlog
   - 2.3 Weitere Scrum-Artefakte und Managementwerkzeuge

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. Requirements Engineering und agiles Architekturmanagement
   - 4.1 Requirements Engineering in agilen Projekten
   - 4.2 Architekturmanagement in agilen Projekten

5. Agiles Testen
   - 5.1 Grundlagen des agilen Testens und Anforderungen an die Qualitätssicherungsorganisation
   - 5.2 Teststufen und Agilität
   - 5.3 Testautomatisierung

6. Continuous Delivery
   - 6.1 Grundlagen und Continuous Delivery Pipeline
   - 6.2 Continuous Build und Continuous Integration
   - 6.3 Akzeptanztests, Lasttests und Continuous Deployment

Literatur

Pflichtliteratur

Weiterführende Literatur

- Cohn, M. (2010). User Stories für die agile Software-Entwicklung mit Scrum, XP u.a. mitp.
- Crispin, L. & Gregory, J. (2008): Agile Testing. A Practical Guide for Testers and Agile Teams. AddisonWesley.
- Kim, G., Humble, J., Debois, P., Willis, J., & Forsgren, N. (2022). Das DevOps-Handbuch. Teams, Tools und Infrastrukturen erfolgreich umgestalten. 2., aktualisierte und erweiterte Auflage. O'Reilly.
- Rubin, K. S. (2014). Essential Scrum. Umfassendes Scrum-Wissen aus der Praxis. mitp.

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Projekt: Agiles DevSecOps-Software-Engineering

Kurscode: DLBCSEEDSO01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
BA	Deutsch		5	DLBWIWTMAS01 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 Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Sicherheit in komplexen Netzwerken

Modulcode: DLBCSEESCN_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof.Dr. Holger Klus (IT-Architekturmanagement) / Prof. Dr. Jörn-Marc Schmidt (Projekt: IT-Sicherheitsarchitekturen)

Kurse im Modul

- IT-Architekturmanagement (IAMG01)
- Projekt: IT-Sicherheitsarchitekturen (DLBCSEESCN01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	IT-Architekturmanagement • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "Kombistudium": Klausur, 90 Minuten Projekt: IT-Sicherheitsarchitekturen • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Duales myStudium": 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	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

IT-Architekturmanagement

Kurscode: IAMG01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

- Beims, M., & Ziegenbein, M. (2023). IT-Service-Management in der Praxis mit ITIL®: Zusammenarbeit systematisieren und relevante Ergebnisse erzielen.
- Hanschke, I. (2022). Enterprise Architecture Management - einfach und effektiv: Ein praktischer Leitfaden für die Einführung von EAM. Carl Hanser Verlag GmbH & Co KG.
- Keuntje, J. H., & Barkow, R. (Hrsg.). (2010). Enterprise Architecture Management in der Praxis: Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen.
- Keller, W. (2017). IT-Unternehmensarchitektur: Von der Geschäftsstrategie zur optimalen IT-Unterstützung. dpunkt.verlag.
- Schwarzer, B. (2009). Einführung in das Enterprise Architecture Management: Verstehen – Planen – Umsetzen. Books on Demand.
- Suhari, D. (2024). Enterprise Architektur entschlüsselt: Ein praxisorientierter Leitfaden von den Grundlagen bis zur Anwendung. Springer-Verlag.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Projekt: IT-Sicherheitsarchitekturen

Kurscode: DLBCSEESCN01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 [zuletzt besucht am 22.08.2020]).

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Network Forensics

Module Code: DLBCSEENF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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

Mohammad Reza Rostami (Protocols, Log- and Dataflow-Analysis in Depth) / Dr. Jetzabel Maritza Serna-Olvera (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

Module Exam

Split Exam

Protocols, Log- and Dataflow-Analysis in Depth

- Study Format "Duales myStudium": Exam, 90 Minutes
- Study Format "myStudies": Exam, 90 Minutes
- Study Format "Distance Learning": Exam, 90 Minutes

Seminar: Threat Hunting, Analysis and Incident Response

- Study Format "Duales myStudium": Written Assessment: Research Essay
- Study Format "Distance Learning": Written Assessment: Research Essay
- Study Format "myStudies": Written Assessment: Research Essay

Weight of Module
see curriculum

Module Contents

Protocols, Log- and Dataflow-Analysis in Depth

- Network Basics
- Operating System Logs
- Packet Capturing and Analysis
- Log Management
- Preparation for Attacks
- Intrusion Detection and Prevention System

Seminar: Threat Hunting, Analysis and Incident Response

- Mitre ATT&CK TTPs
- APT actors
- Security coverage gap analysis

Learning Outcomes

Protocols, Log- and Dataflow-Analysis in Depth

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.

Seminar: Threat Hunting, Analysis and Incident Response

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.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

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 Publicaton 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ 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 Duales myStudium

Study Format	Course Type
Duales myStudium	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Studium Generale I und II

Modulcode: DLBSG

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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)

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 "Duales myStudium": Siehe gewählter Kurs • Studienformat "Fernstudium": Siehe gewählter Kurs • Studienformat "myStudium": Siehe gewählter Kurs Studium Generale II • Studienformat "Kombistudium": Siehe gewählter Kurs • Studienformat "Duales myStudium": 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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist ein eigenständiges Angebot mit möglichen Bezügen zu verschiedenen Pflicht- und Wahlpflichtmodulen	Alle Bachelor-Programme des IU Fernstudiums

Studium Generale I

Kurscode: DLBSG01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Siehe Kursbeschreibung des gewählten Kurses

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat myStudium

Studienform	Kursart
myStudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studium Generale II

Kurscode: DLBSG02

Niveau	Kurs- und Prüfungssprache	SWS	CP	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.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Siehe Kursbeschreibung des gewählten Kurses

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat myStudium

Studienform	Kursart
myStudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

6. Semester

Business Intelligence

Modulcode: IWBI

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Maik Drozdzynski (Business Intelligence) / Anuja Hariharan (Projekt: Business Intelligence)

Kurse im Modul

- Business Intelligence (IWBI01)
- Projekt: Business Intelligence (IWBI02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Business Intelligence • Studienformat "Kombistudium": Klausur, 90 Minuten • Studienformat "myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten (100%) • Studienformat "Duales myStudium": Klausur, 90 Minuten Projekt: Business Intelligence • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht
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	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Business Intelligence

Kurscode: IWBI01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Analysesysteme
5.1 Freie Datenrecherche und OLAP
5.2 Berichtssysteme
5.3 Modellgestützte Analysesysteme
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 [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 Kombistudium

Studienform	Kursart
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Projekt: Business Intelligence

Kurscode: IWBI02

Niveau	Kurs- und Prüfungssprache	SWS	CP	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./Uebernickel, 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.
- Uebernickel, 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

Studienform	**Kursart**
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat myStudium

Studienform	**Kursart**
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Future Threats

Modulcode: DLBCSEEFT_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof. Dr. Björn Kaidel (Threat Modeling) / Prof. Dr. Jörn-Marc Schmidt (Projekt: Threat Modeling)

Kurse im Modul

- Threat Modeling (DLBCSEEFT01_D)
- Projekt: Threat Modeling (DLBCSEEFT02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Threat Modeling • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "myStudium": Klausur, 90 Minuten Projekt: Threat Modeling • Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Threat Modeling

- CIA und mehr
- Messung von Cyber-Bedrohungen
- Threat Modeling
- Angriffsbibliotheken
- Risikomanagement
- 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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

Bezüge zu anderen Modulen im Studiengang	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Threat Modeling

Kurscode: DLBCSEEFT01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. CIA und mehr
   - 1.1 Vertraulichkeit (Confidentiality)
   - 1.2 Integrität (Integrity)
   - 1.3 Verfügbarkeit (Availability)
   - 1.4 Bekannte IT-Sicherheitsprobleme
2. Messung von Cyber-Bedrohungen
   - 2.1 Konzepte zur Messung von Bedrohungen
   - 2.2 Metriken für Cyber-Bedrohung
   - 2.3 Wichtige Cyberangriffe und ihre Auswirkungen
   - 2.4 Black Swan Events
3. Threat Modeling

3.1 Angriffsbaum-Methodik
3.2 STRIDE
3.3 DREAD
3.4 Schmerzpyramide – “Pyramid of Pain”

4. Angriffsbibliotheken
   4.1 CAPEC
   4.2 Soloves Taxonomie der Privatsphäre
   4.3 Modellierung mit Mitre ATT&CK®
   4.4 Identifizierung von Angriffen

5. Risikomanagement
   5.1 Risikomanagement - Ein Überblick
   5.2 Reaktion auf Zwischenfälle und Krisenmanagement
   5.3 Unvorhersehbare Ereignisse (Black Swan Events)
   5.4 Kontinuierliche Neubewertung

6. Threat Mitigation
   6.1 Defensive Taktiken und Technologien
   6.2 Strategien zur Risikominderung
   6.3 Validierung des Abwehrschutzes
   6.4 Sicherheit und Privacy by Design
   6.5 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. / Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Projekt: Threat Modeling

Kurscode: DLBCSEEFT02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01; DLBCSEEFT01_D oder DLBCSEEFT01_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. Speziell im dualen Fernstudium: Im dualen Fernstudium ist der Theorie-Praxis-Transfer anhand eines realen Projekts, das im Praxisbetrieb umgesetzt werden soll, zu leisten. Im Rahmen des Praxisprojektes bearbeiten die Studierenden eine praxisrelevante Fragestellung ihres Praxisbetriebs unter Betreuung einer:s Lehrenden. Eine Betreuung seitens Praxispartner kann auf Wunsch erfolgen.

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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

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 myStudium

Studienform	**Kursart**
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	30 h	0 h	120 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Cloud Security

Module Code: DLBCSEECS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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) / Mohammad Reza Rostami (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 "Duales myStudium": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Security by Design in the Cloud • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": 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	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Security Controls in the Cloud

Course Code: DLBCSEECS01_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 Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Security by Design in the Cloud

Course Code: DLBCSEECS02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_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 Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Vulnerability Analysis and Pentesting

Module Code: DLBCSEEPT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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) / Prof. Dr. Björn Kaidel (Project: Pentesting)

Contributing Courses to Module

- Principles of Ethical Hacking (DLBCSEEPT01_E)
- Project: Pentesting (DLBCSEEPT02_E)

Module Exam Type

Module Exam	Split Exam
	Principles of Ethical Hacking • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes Project: Pentesting • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report

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	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Principles of Ethical Hacking

Course Code: DLBCSEEPT01_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/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Project: Pentesting

Course Code: DLBCSEEPT02_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, DLBCSEEPT01_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/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Industrielle Systemsicherheit

Modulcode: DLBCSEEIST_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof. Dr. Marian Benner-Wickner (Grundlagen der industriellen Softwaretechnik) / Prof. Dr. Jörn-Marc Schmidt (Sicherheit im Internet of Things)

Kurse im Modul

- Grundlagen der industriellen Softwaretechnik (IGIS01)
- Sicherheit im Internet of Things (DLBCSEEIST01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Grundlagen der industriellen Softwaretechnik • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "Duales myStudium": Klausur, 90 Minuten Sicherheit im Internet of Things • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten

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 Internets der Dinge (IoT)
- Angriffe auf das Internet der Dinge
- Security by Design
- Gerätesicherung im Internet der Dinge
- Operative Sicherheit
- Cloud-Sicherheit
- Big Data und 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	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Grundlagen der industriellen Softwaretechnik

Kurscode: IGIS01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Sicherheit im Internet of Things

Kurscode: DLBCSEEIST01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Internets der Dinge (IoT)
   - 1.1 Einführung in das IoT
   - 1.2 Architektur
   - 1.3 Nichtindustrielles Internet der Dinge
   - 1.4 Industrie 4.0 (industrielles IoT)
2. Angriffe auf das Internet der Dinge
   - 2.1 Schwachstellen, Bedrohungen und Risiken
   - 2.2 Cyber-Angriffe und Gegenmaßnahmen
3. Security by Design
   - 3.1 Projektmanagement und der sichere Entwicklungs-Lebenszyklus
   - 3.2 Statisches Testen
   - 3.3 Dynamisches Testen
   - 3.4 DevSecOps

4. Gerätesicherung im Internet der Dinge
   - 4.1 Sicherheitsrisiken
   - 4.2 Design-Ziele

5. Operative Sicherheit
   - 5.1 Informations- und Cybersicherheitsmanagementsystem
   - 5.2 Netzwerksicherheit
   - 5.3 Gerätekonfiguration
   - 5.4 Authentifizierung und Autorisierung

6. Cloud-Sicherheit
   - 6.1 Konzept des Fog-Computings
   - 6.2 Bedrohungen für Cloud-Dienste im Internet der Dinge
   - 6.3 Cloudbasierte Sicherheitsdienste
   - 6.4 Absicherung der Cloud-Lösung

7. Big Data und künstliche Intelligenz
   - 7.1 Grundlagen
   - 7.2 Überwachtes Lernen
   - 7.3 Unüberwachtes 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 Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Cyber Threat Intelligence

Module Code: DLBCSEECTI_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum		WiSe/SoSe	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 "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes Project: Defense against APTs • Study Format "myStudies": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "Duales myStudium": 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 extern 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	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	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 analysist 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. Retrieved from 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. Retrieved from https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LMWhite-Paper-Intel-Driven-Defense.pdf ▪ MISP Project. (n.d.). Retrieved from https://www.misp-project.org/ ▪ Mitre ATT&CK. (n.d.). Retrieved from 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 myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ 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
- 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-semantics.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 myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Telekommunikationsspezifische Bedrohungen

Modulcode: DLBCSEEMT_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof. Dr. Olaf Hänßler (Funk- und Telekommunikationssicherheit) / Prof. Dr. Jörn-Marc Schmidt (Softwarearchitektur mobiler Geräte)

Kurse im Modul

- Funk- und Telekommunikationssicherheit (DLBCSEEMT01_D)
- Softwarearchitektur mobiler Geräte (DLBCSEEMT02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Funk- und Telekommunikationssicherheit • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten Softwarearchitektur mobiler Geräte • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Funk- und Telekommunikationssicherheit

- Überblick über drahtlose Protokolle
- Grundlagen von Drahtlosen Netwerken
- 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	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor -Programme im Bereich IT & Technik

Funk- und Telekommunikationssicherheit

Kurscode: DLBCSEEMT01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
BA	Deutsch		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 Netwerken
   - 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 Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Softwarearchitektur mobiler Geräte

Kurscode: DLBCSEEMT02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Handset Technology Stack
   - 1.1 Hardware
   - 1.2 Firmware
   - 1.3 Betriebssystem
   - 1.4 Anwendungen
   - 1.5 Ökosystem
2. Hardware
   - 2.1 RF-Module
   - 2.2 PDA-Modul
   - 2.3 Trusted Execution Environment

- 2.4 2Biometrische Geräte
- 2.5 Ortungstechnologie

3. Android-Betriebssystem
   - 3.1 Hardware
   - 3.2 Bootloader
   - 3.3 Kernel und Hardware-Abstraktionsschicht
   - 3.4 Sandboxing und Virtualisierung
   - 3.5 Codesignierung

4. Apple iOS-Betriebssystem
   - 4.1 Hardware
   - 4.2 Bootloader
   - 4.3 Kernel und Frameworks
   - 4.4 Sandboxing und Virtualisierung
   - 4.5 Codesignierung

5. Mobile Geräte
   - 5.1 Das Internet der Dinge
   - 5.2 Linux
   - 5.3 RTOS
   - 5.4 Android auf Geräten
   - 5.5 Andere gängige eingebettete Betriebssysteme

6. Software-Ökosysteme und Sicherheit
   - 6.1 Google Play
   - 6.2 Apple App Store
   - 6.3 Sicherheitsanbieter
   - 6.4 Die Rolle der Cloud

7. Bedrohungen bei Mobiltelefonen
   - 7.1 Historische Beispiele für Angriffe auf Mobiltelefone
   - 7.2 Taxonomie der Bedrohungen bei Mobiltelefonen
   - 7.3 Jailbreaking

8. Mobilgeräteverwaltung
   - 8.1 Bedrohungen bei BYOD
   - 8.2 Besondere Bedrohungen bei mobilen Geräten
   - 8.3 Patch- und Richtlinienverwaltung

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 ▪ Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Apple Mobile Solution Development

Modulcode: DLAMSD

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Holger Klus (Apple Mobile Solution Development I) / Prof. Dr. Holger Klus (Apple Mobile Solution Development II)

Kurse im Modul

- Apple Mobile Solution Development I (DLAMSD01)
- Apple Mobile Solution Development II (DLAMSD02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Apple Mobile Solution Development I • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht Apple Mobile Solution Development II • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht
Anteil der Modulnote an der Gesamtnote s. Curriculum	

Lehrinhalt des Moduls

Apple Mobile Solution Development I

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.

Apple Mobile Solution Development II

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.

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 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.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Apple Mobile Solution Development I

Kurscode: DLAMSD01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Folien	☑ Prüfungsleitfaden

Apple Mobile Solution Development II

Kurscode: DLAMSD02

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Folien	☑ Prüfungsleitfaden

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studium Generale III und IV

Modulcode: DLBSGDUV

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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)

N.N. (Studium Generale III) / N.N. (Studium Generale IV)

Kurse im Modul

- Studium Generale III (DLBSG03)
- Studium Generale IV (DLBSG04)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Studium Generale III • Studienformat "Duales myStudium": Siehe gewählter Kurs • Studienformat "Fernstudium": Siehe gewählter Kurs Studium Generale IV • Studienformat "Duales myStudium": Siehe gewählter Kurs • Studienformat "Fernstudium": Siehe gewählter Kurs

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Studium Generale III

Als Kurs für das „Studium Generale“ sind prinzipiell alle IU-Bachelorkurse wählbar, sodass inhaltlich aus der gesamten Breite des IU Fernstudiums gewählt werden kann.

Studium Generale IV

Als Kurs für das „Studium Generale“ sind prinzipiell alle IU-Bachelorkurse wählbar, sodass inhaltlich aus der gesamten Breite des IU Fernstudiums gewählt werden kann.

Qualifikationsziele des Moduls

Studium Generale III

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 IV

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist ein eigenständiges Angebot mit möglichen Bezügen zu verschiedenen Pflicht- und Wahlpflichtmodulen	Alle Bachelor-Programme des IU Fernstudiums

Studium Generale III

Kurscode: DLBSG03

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

Beschreibung des Kurses

Im Rahmen des Kurses „Studium Generale III“ 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 III“ 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 wählbar 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.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Siehe Kursbeschreibung des gewählten Kurses

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studium Generale IV

Kurscode: DLBSG04

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

Beschreibung des Kurses

Im Rahmen des Kurses „Studium Generale IV“ 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 IV“ 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 wählbar 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.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Siehe Kursbeschreibung des gewählten Kurses

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

IT-Sicherheitsberatung

Modulcode: DLBCSEEISC_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Rainer Lukas (Technische und betriebliche IT-Sicherheitskonzeptionen) / Nils Kannengießer (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 "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "myStudium": Klausur, 90 Minuten Projekt: Einsatz und Konfiguration von SIEM-Systemen • Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Duales myStudium": 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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Technische und betriebliche IT-Sicherheitskonzeptionen

Kurscode: DLBCSEEISC01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Datenfluss, Interdependenzen und Interrelationen
   - 1.3 Überprüfung und Erkennen von Schwachstellen
   - 1.4 Unterstützende Tools und Techniken

2. Schutzprofile
   - 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 und Sensoren
   - 3.3 Analytik
   - 3.4 Indicators of Compromise - Indikatoren für Kompromittierungen

4. Netzwerküberwachung
   - 4.1 Advanced Threat Protection (ATP)
   - 4.2 Technologie drahtloser Sensornetzwerke
   - 4.3 Austausch von Bedrohungsinformationen

5. Sicherheitsinformationen und Ereignismanagement (SIEM)
   - 5.1 Technische und betriebliche Datenquellen
   - 5.2 Datenfusion
   - 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-Sicherheitsmetriken
   - 6.2 Bewertung der IT-Sicherheit

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Bundesamt für Sicherheit in der Informationstechnik. (2023). BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen. ▪ Eckert, C. (2018). IT-Sicherheit: Konzepte – Verfahren – Protokolle (10. Aufl.). De Gruyter Oldenbourg. ▪ Kappes, M. (2022). Netzwerk- und Datensicherheit: Eine praktische Einführung. Springer Fachmedien. ▪ Kloep, P., & Weigel, K. (2023). Sichere Windows-Infrastrukturen: Das Handbuch für Administratoren. Rheinwerk Computing. ▪ Wendzel, S. (2018). IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung. Springer Fachmedien.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Projekt: Einsatz und Konfiguration von SIEM-Systemen

Kurscode: DLBCSEEISC02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Speziell im dualen Fernstudium: Im dualen Fernstudium ist der Theorie-Praxis-Transfer anhand eines realen Projekts, das im Praxisbetrieb umgesetzt werden soll, zu leisten. Im Rahmen des Praxisprojektes bearbeiten die Studierenden eine praxisrelevante Fragestellung ihres Praxisbetriebs unter Betreuung einer:s Lehrenden. Eine Betreuung seitens Praxispartner kann auf Wunsch erfolgen.

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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

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
- 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 myStudium

Studienform	Kursart
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	30 h	0 h	120 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Folien

Prüfungsvorbereitung
- ☑ Prüfungsleitfaden

Social Engineering

Modulcode: DLBCSEESE_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Nils Kannengießer (Social Engineering und Insider Threats) / Rami Alkubaty (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 "myStudium": Schriftliche Ausarbeitung: Fallstudie • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Fallstudie • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Fallstudie Projekt: Social Engineering • Studienformat "Duales myStudium": Projektpräsentation • Studienformat "Fernstudium": Projektpräsentation • Studienformat "myStudium": 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 Internetdienstanbietern zusammenzuarbeiten.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Social Engineering und Insider Threats

Kurscode: DLBCSEESE01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 so genannten "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 Quidproquo, Köder (Baiting), Medienköder (Media Dropping)
   - 1.3 Scareware, Betrugsmasche CEO-Fraud (CEO-Betrug)
   - 1.4 Pretexting, Tailgating
2. Rechtliche Aspekte des Social Engineering
   - 2.1 Compliance, Verhaltenskodex
   - 2.2 Identitätsdiebstahl
   - 2.3 Datenschutz
3. Erkennung von Insider-Bedrohungen
   - 3.1 Data-Mining-Techniken
   - 3.2 Anwendung von Methoden des Machine Learning
   - 3.3 Umfassendes Framework für die Erkennung von und Reaktion auf Insider-Bedrohungen
   - 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 und internationale Zusammenarbeit sowie 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) sowie 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 myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Projekt: Social Engineering

Kurscode: DLBCSEESE02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Speziell im dualen Fernstudium: Im dualen Fernstudium ist der Theorie-Praxis-Transfer anhand eines realen Projekts, das im Praxisbetrieb umgesetzt werden soll, zu leisten. Im Rahmen des Praxisprojektes bearbeiten die Studierenden eine praxisrelevante Fragestellung ihres Praxisbetriebs unter Betreuung einer:s Lehrenden. Eine Betreuung seitens Praxispartner kann auf Wunsch erfolgen.

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 Internetdienstanbietern zusammenzuarbeiten.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

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 Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Projektpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	30 h	0 h	120 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Projektpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat myStudium

Studienform	**Kursart**
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Projektpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Host Forensics

Module Code: DLBCSEEHF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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

Mohammad Reza Rostami (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 • Study Format "myStudies": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes Seminar: Sandbox Interpretation • Study Format "myStudies": Written Assessment: Research Essay • Study Format "Duales myStudium": Written Assessment: Research Essay • 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	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	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 Understanding Malware: Components, Types, and Analysis
    - 1.2 Forensics
    - 1.3 Root Cause Analysis
    - 1.4 The MITRE Attack Framework
    - 1.5 Best Practices for Malware Prevention and Mitigation
2. Analysis Lab Setup
    - 2.1 Building a Secure Malware Analysis Lab
    - 2.2 Stealth
    - 2.3 Isolation
    - 2.4 Honeypots
3. Tools of the Trade
    - 3.1 Virtual Machines
    - 3.2 Debugger
    - 3.3 Anti Debugging Mechanism
    - 3.4 Disassembler

4. Malware Classification
   - 4.1 Malware Triage and Classification
   - 4.2 Structure of a Virus
   - 4.3 Antivirus
   - 4.4 VirusTotal
   - 4.5 Yara
   - 4.6 AI-assisted Malware Analysis

5. Sandboxes
   - 5.1 Different Sandbox Concepts and Their Purposes
   - 5.2 Levels of Interaction
   - 5.3 Instrumentation
   - 5.4 Online Sandboxing Services
   - 5.5 Sandbox Detection and Evasion

6. Reversing
   - 6.1 Understanding Malware Analysis and Its Impact
   - 6.2 Unpacking, Decrypting, and De-Obfuscation
   - 6.3 Debugging Techniques
   - 6.4 Control Flow Analysis
   - 6.5 Library and System Calls

7. Digging Deeper
   - 7.1 Threat Intelligence Integration
   - 7.2 Analysis of JavaScript Code
   - 7.3 Memory Forensics
   - 7.4 Understanding and Debugging Rootkits

Literature

Compulsory Reading

Further Reading

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

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ 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 myStudies

Study Format	Course Type
myStudies	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

DevSecOps

Modulcode: DLBCSEEDSO-01_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		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) / Prof. Dr. Jörn-Marc Schmidt (Projekt: Agiles DevSecOps-Software-Engineering)

Kurse im Modul

- Techniken und Methoden der agilen Softwareentwicklung (DLBWIWTMAS01)
- Projekt: Agiles DevSecOps-Software-Engineering (DLBCSEEDSO01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Techniken und Methoden der agilen Softwareentwicklung • Studienformat "Kombistudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "myStudium": Klausur, 90 Minuten • Studienformat "Duales myStudium": Klausur, 90 Minuten Projekt: Agiles DevSecOps-Software-Engineering • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • 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
- Agile Softwareentwicklung mit Scrum
- Agiles Portfolio- und Projektmanagement
- Requirements Engineering und agiles Architekturmanagement
- Agiles Testen
- Continuous Delivery

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,

- den Ansatz der agilen Softwareentwicklung zu charakterisieren und gegenüber der klassischen Softwareentwicklung abzugrenzen.
- den allgemeinen Aufbau und Ablauf eines Scrum-Projekts zu beschreiben.
- agile Techniken zur Durchführung der Kernaktivitäten des Software-Engineering zu erläutern und diese anzuwenden.
- die Methoden und Werkzeuge des Continuous-Delivery-Ansatzes zu erklären und die Relevanz des Ansatzes im Unternehmenskontext zu beurteilen.

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	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Techniken und Methoden der agilen Softwareentwicklung

Kurscode: DLBWIWTMAS01

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

Beschreibung des Kurses

Der Kurs vermittelt den Studierenden einen umfassenden Einblick in die agile Softwareentwicklung. Hierbei werden sowohl die grundlegenden agilen Prinzipien dargestellt als auch deren Anwendung im Kontext von kleinen und großen Softwareentwicklungsprojekten. Anhand praktischer Beispiele lernen die Studierenden agile Techniken zur Durchführung der Kernaktivitäten im Software-Engineering kennen. Als besonderer Schwerpunkt wird dabei auch auf den Ansatz des Continuous Delivery eingegangen und dessen Methoden und Werkzeuge vorgestellt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Ansatz der agilen Softwareentwicklung zu charakterisieren und gegenüber der klassischen Softwareentwicklung abzugrenzen.
- den allgemeinen Aufbau und Ablauf eines Scrum-Projekts zu beschreiben.
- agile Techniken zur Durchführung der Kernaktivitäten des Software-Engineering zu erläutern und diese anzuwenden.
- die Methoden und Werkzeuge des Continuous-Delivery-Ansatzes zu erklären und die Relevanz des Ansatzes im Unternehmenskontext zu beurteilen.

Kursinhalt

1. Merkmale und Prinzipien von Agilität
   - 1.1 Merkmale und Herausforderungen von Softwareprojekten
   - 1.2 Klassifikationen von Unsicherheit
   - 1.3 Gegenüberstellung von agiler und klassischer Softwareentwicklung
   - 1.4 Prinzipien der Agilität
2. Agile Softwareentwicklung mit Scrum
   - 2.1 Grundlagen und allgemeiner Aufbau von Scrum
   - 2.2 Zentrales Managementartefakt: Product Backlog
   - 2.3 Weitere Scrum-Artefakte und Managementwerkzeuge

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. Requirements Engineering und agiles Architekturmanagement
   - 4.1 Requirements Engineering in agilen Projekten
   - 4.2 Architekturmanagement in agilen Projekten

5. Agiles Testen
   - 5.1 Grundlagen des agilen Testens und Anforderungen an die Qualitätssicherungsorganisation
   - 5.2 Teststufen und Agilität
   - 5.3 Testautomatisierung

6. Continuous Delivery
   - 6.1 Grundlagen und Continuous Delivery Pipeline
   - 6.2 Continuous Build und Continuous Integration
   - 6.3 Akzeptanztests, Lasttests und Continuous Deployment

Literatur

Pflichtliteratur

Weiterführende Literatur

- Cohn, M. (2010). User Stories für die agile Software-Entwicklung mit Scrum, XP u.a. mitp.
- Crispin, L. & Gregory, J. (2008): Agile Testing. A Practical Guide for Testers and Agile Teams. AddisonWesley.
- Kim, G., Humble, J., Debois, P., Willis, J., & Forsgren, N. (2022). Das DevOps-Handbuch. Teams, Tools und Infrastrukturen erfolgreich umgestalten. 2., aktualisierte und erweiterte Auflage. O'Reilly.
- Rubin, K. S. (2014). Essential Scrum. Umfassendes Scrum-Wissen aus der Praxis. mitp.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Studienformat myStudium

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Projekt: Agiles DevSecOps-Software-Engineering

Kurscode: DLBCSEEDSO01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
BA	Deutsch		5	DLBWIWTMAS01 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 Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Sicherheit in komplexen Netzwerken

Modulcode: DLBCSEESCN_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof.Dr. Holger Klus (IT-Architekturmanagement) / Prof. Dr. Jörn-Marc Schmidt (Projekt: IT-Sicherheitsarchitekturen)

Kurse im Modul

- IT-Architekturmanagement (IAMG01)
- Projekt: IT-Sicherheitsarchitekturen (DLBCSEESCN01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	IT-Architekturmanagement • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "Kombistudium": Klausur, 90 Minuten Projekt: IT-Sicherheitsarchitekturen • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Duales myStudium": 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	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

IT-Architekturmanagement

Kurscode: IAMG01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

- Beims, M., & Ziegenbein, M. (2023). IT-Service-Management in der Praxis mit ITIL®: Zusammenarbeit systematisieren und relevante Ergebnisse erzielen.
- Hanschke, I. (2022). Enterprise Architecture Management - einfach und effektiv: Ein praktischer Leitfaden für die Einführung von EAM. Carl Hanser Verlag GmbH & Co KG.
- Keuntje, J. H., & Barkow, R. (Hrsg.). (2010). Enterprise Architecture Management in der Praxis: Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen.
- Keller, W. (2017). IT-Unternehmensarchitektur: Von der Geschäftsstrategie zur optimalen IT-Unterstützung. dpunkt.verlag.
- Schwarzer, B. (2009). Einführung in das Enterprise Architecture Management: Verstehen – Planen – Umsetzen. Books on Demand.
- Suhari, D. (2024). Enterprise Architektur entschlüsselt: Ein praxisorientierter Leitfaden von den Grundlagen bis zur Anwendung. Springer-Verlag.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Projekt: IT-Sicherheitsarchitekturen

Kurscode: DLBCSEESCN01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 [zuletzt besucht am 22.08.2020]).

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Network Forensics

Module Code: DLBCSEENF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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

Mohammad Reza Rostami (Protocols, Log- and Dataflow-Analysis in Depth) / Dr. Jetzabel Maritza Serna-Olvera (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

Module Exam

Split Exam

Protocols, Log- and Dataflow-Analysis in Depth

- Study Format "Duales myStudium": Exam, 90 Minutes
- Study Format "myStudies": Exam, 90 Minutes
- Study Format "Distance Learning": Exam, 90 Minutes

Seminar: Threat Hunting, Analysis and Incident Response

- Study Format "Duales myStudium": Written Assessment: Research Essay
- Study Format "Distance Learning": Written Assessment: Research Essay
- Study Format "myStudies": Written Assessment: Research Essay

Weight of Module
see curriculum

Module Contents

Protocols, Log- and Dataflow-Analysis in Depth

- Network Basics
- Operating System Logs
- Packet Capturing and Analysis
- Log Management
- Preparation for Attacks
- Intrusion Detection and Prevention System

Seminar: Threat Hunting, Analysis and Incident Response

- Mitre ATT&CK TTPs
- APT actors
- Security coverage gap analysis

Learning Outcomes

Protocols, Log- and Dataflow-Analysis in Depth

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.

Seminar: Threat Hunting, Analysis and Incident Response

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.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

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 Publicaton 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	**Course Type**
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ 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 Duales myStudium

Study Format	Course Type
Duales myStudium	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Business Intelligence

Modulcode: IWBI

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Maik Drozdzynski (Business Intelligence) / Anuja Hariharan (Projekt: Business Intelligence)

Kurse im Modul

- Business Intelligence (IWBI01)
- Projekt: Business Intelligence (IWBI02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Business Intelligence • Studienformat "Kombistudium": Klausur, 90 Minuten • Studienformat "myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten (100%) • Studienformat "Duales myStudium": Klausur, 90 Minuten Projekt: Business Intelligence • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht
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	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Business Intelligence

Kurscode: IWBI01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Analysesysteme
   - 5.1 Freie Datenrecherche und OLAP
   - 5.2 Berichtssysteme
   - 5.3 Modellgestützte Analysesysteme
   - 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 [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 Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Projekt: Business Intelligence

Kurscode: IWBI02

Niveau	Kurs- und Prüfungssprache	SWS	CP	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./Uebernickel, 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.
- Uebernickel, 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

Studienform	**Kursart**
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat myStudium

Studienform	**Kursart**
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Future Threats

Modulcode: DLBCSEEFT_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof. Dr. Björn Kaidel (Threat Modeling) / Prof. Dr. Jörn-Marc Schmidt (Projekt: Threat Modeling)

Kurse im Modul

- Threat Modeling (DLBCSEEFT01_D)
- Projekt: Threat Modeling (DLBCSEEFT02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Threat Modeling • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "myStudium": Klausur, 90 Minuten Projekt: Threat Modeling • Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Threat Modeling

- CIA und mehr
- Messung von Cyber-Bedrohungen
- Threat Modeling
- Angriffsbibliotheken
- Risikomanagement
- 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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

Bezüge zu anderen Modulen im Studiengang	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Threat Modeling

Kurscode: DLBCSEEFT01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. CIA und mehr
   - 1.1 Vertraulichkeit (Confidentiality)
   - 1.2 Integrität (Integrity)
   - 1.3 Verfügbarkeit (Availability)
   - 1.4 Bekannte IT-Sicherheitsprobleme
2. Messung von Cyber-Bedrohungen
   - 2.1 Konzepte zur Messung von Bedrohungen
   - 2.2 Metriken für Cyber-Bedrohung
   - 2.3 Wichtige Cyberangriffe und ihre Auswirkungen
   - 2.4 Black Swan Events
3. Threat Modeling

3.1 Angriffsbaum-Methodik
3.2 STRIDE
3.3 DREAD
3.4 Schmerzpyramide – “Pyramid of Pain”

4. Angriffsbibliotheken
   4.1 CAPEC
   4.2 Soloves Taxonomie der Privatsphäre
   4.3 Modellierung mit Mitre ATT&CK®
   4.4 Identifizierung von Angriffen

5. Risikomanagement
   5.1 Risikomanagement - Ein Überblick
   5.2 Reaktion auf Zwischenfälle und Krisenmanagement
   5.3 Unvorhersehbare Ereignisse (Black Swan Events)
   5.4 Kontinuierliche Neubewertung

6. Threat Mitigation
   6.1 Defensive Taktiken und Technologien
   6.2 Strategien zur Risikominderung
   6.3 Validierung des Abwehrschutzes
   6.4 Sicherheit und Privacy by Design
   6.5 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. / Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Projekt: Threat Modeling

Kurscode: DLBCSEEFT02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01; DLBCSEEFT01_D oder DLBCSEEFT01_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. Speziell im dualen Fernstudium: Im dualen Fernstudium ist der Theorie-Praxis-Transfer anhand eines realen Projekts, das im Praxisbetrieb umgesetzt werden soll, zu leisten. Im Rahmen des Praxisprojektes bearbeiten die Studierenden eine praxisrelevante Fragestellung ihres Praxisbetriebs unter Betreuung einer:s Lehrenden. Eine Betreuung seitens Praxispartner kann auf Wunsch erfolgen.

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.
- Speziell im dualen Fernstudium:
- das im Studium bisher erworbene Wissen auf praktische Probleme anzuwenden und durch praktische Erfahrungen im Unternehmen zu erweitern.
- instruktive Beobachtungen und Erfahrungen im Handeln zu machen.

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 myStudium

Studienform	Kursart
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	30 h	0 h	120 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Folien	☑ Prüfungsleitfaden
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Cloud Security

Module Code: DLBCSEECS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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) / Mohammad Reza Rostami (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 "Duales myStudium": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes Project: Security by Design in the Cloud • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": 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	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Security Controls in the Cloud

Course Code: DLBCSEECS01_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 Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Slides	

Project: Security by Design in the Cloud

Course Code: DLBCSEECS02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_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 Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Vulnerability Analysis and Pentesting

Module Code: DLBCSEEPT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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) / Prof. Dr. Björn Kaidel (Project: Pentesting)

Contributing Courses to Module

- Principles of Ethical Hacking (DLBCSEEPT01_E)
- Project: Pentesting (DLBCSEEPT02_E)

Module Exam Type

Module Exam	Split Exam
	Principles of Ethical Hacking • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes • Study Format "myStudies": Exam, 90 Minutes Project: Pentesting • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report

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	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Principles of Ethical Hacking

Course Code: DLBCSEEPT01_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/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Project: Pentesting

Course Code: DLBCSEEPT02_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, DLBCSEEPT01_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/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Industrielle Systemsicherheit

Modulcode: DLBCSEEIST_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof. Dr. Marian Benner-Wickner (Grundlagen der industriellen Softwaretechnik) / Prof. Dr. Jörn-Marc Schmidt (Sicherheit im Internet of Things)

Kurse im Modul

- Grundlagen der industriellen Softwaretechnik (IGIS01)
- Sicherheit im Internet of Things (DLBCSEEIST01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Grundlagen der industriellen Softwaretechnik • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "Duales myStudium": Klausur, 90 Minuten Sicherheit im Internet of Things • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten

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 Internets der Dinge (IoT)
- Angriffe auf das Internet der Dinge
- Security by Design
- Gerätesicherung im Internet der Dinge
- Operative Sicherheit
- Cloud-Sicherheit
- Big Data und 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	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Grundlagen der industriellen Softwaretechnik

Kurscode: IGIS01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Sicherheit im Internet of Things

Kurscode: DLBCSEEIST01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Internets der Dinge (IoT)
   - 1.1 Einführung in das IoT
   - 1.2 Architektur
   - 1.3 Nichtindustrielles Internet der Dinge
   - 1.4 Industrie 4.0 (industrielles IoT)
2. Angriffe auf das Internet der Dinge
   - 2.1 Schwachstellen, Bedrohungen und Risiken
   - 2.2 Cyber-Angriffe und Gegenmaßnahmen
3. Security by Design
   - 3.1 Projektmanagement und der sichere Entwicklungs-Lebenszyklus
   - 3.2 Statisches Testen
   - 3.3 Dynamisches Testen
   - 3.4 DevSecOps

4. Gerätesicherung im Internet der Dinge
   - 4.1 Sicherheitsrisiken
   - 4.2 Design-Ziele

5. Operative Sicherheit
   - 5.1 Informations- und Cybersicherheitsmanagementsystem
   - 5.2 Netzwerksicherheit
   - 5.3 Gerätekonfiguration
   - 5.4 Authentifizierung und Autorisierung

6. Cloud-Sicherheit
   - 6.1 Konzept des Fog-Computings
   - 6.2 Bedrohungen für Cloud-Dienste im Internet der Dinge
   - 6.3 Cloudbasierte Sicherheitsdienste
   - 6.4 Absicherung der Cloud-Lösung

7. Big Data und künstliche Intelligenz
   - 7.1 Grundlagen
   - 7.2 Überwachtes Lernen
   - 7.3 Unüberwachtes 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 Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Cyber Threat Intelligence

Module Code: DLBCSEECTI_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum		WiSe/SoSe	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 "myStudies": Exam, 90 Minutes • Study Format "Distance Learning": Exam, 90 Minutes • Study Format "Duales myStudium": Exam, 90 Minutes Project: Defense against APTs • Study Format "myStudies": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "Duales myStudium": 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 extern 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	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	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 analysist 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. Retrieved from 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. Retrieved from https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LMWhite-Paper-Intel-Driven-Defense.pdf ▪ MISP Project. (n.d.). Retrieved from https://www.misp-project.org/ ▪ Mitre ATT&CK. (n.d.). Retrieved from 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 myStudies

Study Format	Course Type
myStudies	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support	Learning Material	Exam Preparation
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ 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
- 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-semantics.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 myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Telekommunikationsspezifische Bedrohungen

Modulcode: DLBCSEEMT_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof. Dr. Olaf Hänßler (Funk- und Telekommunikationssicherheit) / Prof. Dr. Jörn-Marc Schmidt (Softwarearchitektur mobiler Geräte)

Kurse im Modul

- Funk- und Telekommunikationssicherheit (DLBCSEEMT01_D)
- Softwarearchitektur mobiler Geräte (DLBCSEEMT02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Funk- und Telekommunikationssicherheit • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten Softwarearchitektur mobiler Geräte • Studienformat "Duales myStudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Funk- und Telekommunikationssicherheit

- Überblick über drahtlose Protokolle
- Grundlagen von Drahtlosen Netwerken
- 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	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor -Programme im Bereich IT & Technik

Funk- und Telekommunikationssicherheit

Kurscode: DLBCSEEMT01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
BA	Deutsch		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 Netwerken
   - 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 Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Softwarearchitektur mobiler Geräte

Kurscode: DLBCSEEMT02_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Handset Technology Stack
   - 1.1 Hardware
   - 1.2 Firmware
   - 1.3 Betriebssystem
   - 1.4 Anwendungen
   - 1.5 Ökosystem
2. Hardware
   - 2.1 RF-Module
   - 2.2 PDA-Modul
   - 2.3 Trusted Execution Environment

- 2.4 2Biometrische Geräte
- 2.5 Ortungstechnologie

3. Android-Betriebssystem
   - 3.1 Hardware
   - 3.2 Bootloader
   - 3.3 Kernel und Hardware-Abstraktionsschicht
   - 3.4 Sandboxing und Virtualisierung
   - 3.5 Codesignierung

4. Apple iOS-Betriebssystem
   - 4.1 Hardware
   - 4.2 Bootloader
   - 4.3 Kernel und Frameworks
   - 4.4 Sandboxing und Virtualisierung
   - 4.5 Codesignierung

5. Mobile Geräte
   - 5.1 Das Internet der Dinge
   - 5.2 Linux
   - 5.3 RTOS
   - 5.4 Android auf Geräten
   - 5.5 Andere gängige eingebettete Betriebssysteme

6. Software-Ökosysteme und Sicherheit
   - 6.1 Google Play
   - 6.2 Apple App Store
   - 6.3 Sicherheitsanbieter
   - 6.4 Die Rolle der Cloud

7. Bedrohungen bei Mobiltelefonen
   - 7.1 Historische Beispiele für Angriffe auf Mobiltelefone
   - 7.2 Taxonomie der Bedrohungen bei Mobiltelefonen
   - 7.3 Jailbreaking

8. Mobilgeräteverwaltung
   - 8.1 Bedrohungen bei BYOD
   - 8.2 Besondere Bedrohungen bei mobilen Geräten
   - 8.3 Patch- und Richtlinienverwaltung

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 ▪ Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Supply Chain Management

Modulcode: BWSC

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Dr. Guido Schmidt (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)

Modulprüfung	Teilmodulprüfung
	Supply-Chain-Management I • Studienformat "Fernstudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten • Studienformat "Duales myStudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten • Studienformat "myStudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten • Studienformat "Kombistudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten Supply-Chain-Management II • Studienformat "myStudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, • Studienformat "Kombistudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten • Studienformat "Fernstudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten • Studienformat "Duales myStudium": Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten
Anteil der Modulnote an der Gesamtnote s. Curriculum	

Lehrinhalt des Moduls

Supply-Chain-Management I

- Historische und terminologische Aspekte zum SCM-Konzept
- Entstehungsmotive von unternehmensübergreifenden Wertschöpfungsnetzwerken
- Gestaltungsprinzipien und Effekte von Wertschöpfungsnetzwerken
- Logistische Kernprozesse und SCM
- Informationstechnische Aspekte des SCM-Konzeptes
- Koordination und Kollaboration der Netzwerkpartner
- Branchenspezifische Lösungen des SCM

Supply-Chain-Management II

- Strategische Aspekte des SCMs
- SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Planung
- SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Beschaffung
- SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Produktion
- SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Distribution

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	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Transport & Logistik auf	Alle Bachelor-Programme im Bereich Transport & Logistik

Supply-Chain-Management I

Kurscode: BWSC01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Grundlangen
- 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

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden	
Lernmaterial	**Prüfungsvorbereitung**
☑ Skript	☑ Musterklausur
☑ Video	☑ Online Tests
☑ Audio	☑ Prüfungsleitfaden
☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden	
Lernmaterial	**Prüfungsvorbereitung**
☑ Skript	☑ Musterklausur
☑ Video	☑ Online Tests
☑ Audio	☑ Prüfungsleitfaden
☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden	
Lernmaterial	**Prüfungsvorbereitung**
☑ Skript	☑ Online Tests

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden	
Lernmaterial	**Prüfungsvorbereitung**
☑ Skript	☑ Online Tests

Supply-Chain-Management II

Kurscode: BWSC02

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Peplenishment
   - 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

Studienform	**Kursart**
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	☑ Prüfungsleitfaden
	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	☑ Prüfungsleitfaden
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	☑ Prüfungsleitfaden
	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur oder Schriftliche Ausarbeitung: Hausarbeit, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
100 h	0 h	25 h	25 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	☑ Prüfungsleitfaden
	☑ Folien	

Angewandte Smart Factory

Modulcode: DLBINGASF

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Christian Magnus (Smart Factory) / Prof. Dr. Matthias Eifler (Projekt: Smart Devices & Factory)

Kurse im Modul

- Smart Factory (DLBINGSF01)
- Projekt: Smart Devices & Factory (DLBINGPSDF01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Smart Factory • Studienformat "Fernstudium": Klausur, 90 Minuten (100%) • Studienformat "Duales myStudium": Klausur, 90 Minuten Projekt: Smart Devices & Factory • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht (100%)

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Smart Factory

- Motivation und Begriffsabgrenzung
- Entwicklung der Automatisierung
- Technologische Grundlagen und Standards
- Grundkonzepte einer Smart Factory
- Referenzarchitekturen
- Smart Factory Engineering
- Sicherheit

Projekt: Smart Devices & Factory

Qualifikationsziele des Moduls

Smart Factory

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.

Projekt: Smart Devices & Factory

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Technologien und Standards im Kontext Smart Devices & Factory zu durchdringen und ein vertieftes Verständnis für diese zu besitzen.
- Technologien im Kontext Smart Devices & Factory an einem einfachen Praxisbeispiel anwenden zu können.
- zu einer ausgewählten Aufgabenstellung einen Hardware- oder Software-Prototypen entwerfen zu können.
- Entwurfs- und Entwicklungstätigkeiten dokumentieren zu können.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Smart Factory

Kurscode: DLBINGSF01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 smarter 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./Hompel, 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.
- Haupert, 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 Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Audio
- ☑ Folien

Prüfungsvorbereitung
- ☑ Musterklausur
- ☑ Online Tests

Projekt: Smart Devices & Factory

Kurscode: DLBINGPSDF01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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. Mit Hilfe einer passenden Prototyping-Umgebung, sei es Hardware wie Prototyping-Boards oder Software wie technologiespezifische Entwicklungsumgebungen, bearbeiten sie die Aufgabe. Dabei setzen sie grundlegende Konzepte, Methoden und Werkzeuge aus den Bereichen Smart Devices und Smart Factory an. Zum Abschluss dokumentieren sie ihre Ergebnisse.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Technologien und Standards im Kontext Smart Devices & Factory zu durchdringen und ein vertieftes Verständnis für diese zu besitzen.
- Technologien im Kontext Smart Devices & Factory an einem einfachen Praxisbeispiel anwenden zu können.
- zu einer ausgewählten Aufgabenstellung einen Hardware- oder Software-Prototypen entwerfen zu können.
- Entwurfs- und Entwicklungstätigkeiten dokumentieren zu können.

Kursinhalt

- Ein Katalog mit den jeweils aktuell bereitgestellten Aufgabenstellungen wird auf der Online-Plattform des Kurses bereitgestellt. Er bietet die inhaltliche Basis und kann fortlaufend ergänzt bzw. aktualisiert werden.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Themenspezifische Literaturauswahl

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Robotics und Automatisierung

Modulcode: DLBCSDWRA

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Hans Kristian Kerwat (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 & Präsentation (best. / nicht best.), 90 Minuten • Studienformat "Kombistudium": Klausur & Präsentation (best. / nicht best.), 90 Minuten • Studienformat "myStudium": Klausur & Präsentation (best. / nicht best.), 90 Minuten • Studienformat "Duales myStudium": Klausur & Präsentation (best. / nicht best.), 90 Minuten Automatisierung und Robotics • Studienformat "Kombistudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "Duales myStudium": 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	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Ingenieurswissenschaften und Informatik & Software-Entwicklung auf.	Alle Bachelor-Programme im Bereich IT & Technik.

Fertigungsverfahren Industrie 4.0

Kurscode: DLBINGFVI01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

Studienform	Kursart
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur & Präsentation (best. / nicht best.), 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur & Präsentation (best. / nicht best.), 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur & Präsentation (best. / nicht best.), 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur & Präsentation (best. / nicht best.), 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Automatisierung und Robotics

Kurscode: DLBINGAUR01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Temparatursensoren
- 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

Studienform	Kursart
Kombistudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Folien	

Mobile Software Engineering

Modulcode: DLBCSEMSE_D

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Marian Benner-Wickner (Mobile Software Engineering) / Prof. Dr. Marian Benner-Wickner (Projekt: Mobile Software Engineering)

Kurse im Modul

- Mobile Software Engineering (DLBCSEMSE01_D)
- Projekt: Mobile Software Engineering (DLBCSEMSE02_D)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Mobile Software Engineering

- Studienformat "myStudium": Klausur, 90 Minuten
- Studienformat "Fernstudium": Klausur, 90 Minuten
- Studienformat "Duales myStudium": Klausur, 90 Minuten

Projekt: Mobile Software Engineering

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht
- Studienformat "myStudium": Schriftliche Ausarbeitung: Projektbericht
- Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Mobile Software Engineering

- Grundlagen der mobilen Softwareentwicklung
- Android-Systemarchitektur
- Entwicklungsumgebung
- Kernkomponenten einer Android-App
- Interaktion zwischen Anwendungskomponenten
- Fortgeschrittene Techniken

Projekt: Mobile Software Engineering

In diesem Modul beschäftigen sich die Studierenden mit der Konzeption, Umsetzung und Dokumentation von kleinen, mobilen Anwendungen auf Basis einer konkreten Aufgabenstellung.

Qualifikationsziele des Moduls

Mobile Software Engineering

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Unterschiede und Besonderheiten der Softwareentwicklung für mobile Systeme zu erkennen und zu erklären.
- zwischen verschiedenen Aktivitäten, Rollen und Risiken bei der Erstellung, dem Betrieb und der Wartung von mobilen Softwaresystemen zu unterscheiden.
- die Architektur und die technischen Merkmale der Android-Plattform zu erklären und zu unterscheiden.
- selbständig mobile Softwaresysteme zur Lösung konkreter Probleme für die "Android"-Plattform zu erstellen.

Projekt: Mobile Software Engineering

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbständig einen Prototyp einer kleinen mobilen Anwendung zur Lösung eines bestimmten Problems zu entwerfen und zu erstellen.
- typische Probleme und Herausforderungen bei der praktischen Umsetzung von kleinen mobilen Anwendungen zu erkennen.
- die Konzeption und Umsetzung kleiner, eigenständig implementierter mobiler Anwendungen zu dokumentieren.

Bezüge zu anderen Modulen im Studiengang	Bezüge zu anderen Studiengängen der Hochschule
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Mobile Software Engineering

Kurscode: DLBCSEMSE01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 rein webbasierter Softwaresysteme unterscheidet, welche Technologien und Programmierkonzepte typischerweise zum Einsatz kommen und welche typischen Herausforderungen es bei der App-Entwicklung für professionelle Anwendungen gibt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Unterschiede und Besonderheiten der Softwareentwicklung für mobile Systeme zu erkennen und zu erklären.
- zwischen verschiedenen Aktivitäten, Rollen und Risiken bei der Erstellung, dem Betrieb und der Wartung von mobilen Softwaresystemen zu unterscheiden.
- die Architektur und die technischen Merkmale der Android-Plattform zu erklären und zu unterscheiden.
- selbständig mobile Softwaresysteme zur Lösung konkreter Probleme für die "Android"-Plattform zu erstellen.

Kursinhalt

1. Grundlagen der mobilen Softwareentwicklung
   - 1.1 Besondere Eigenschaften von Mobilgeräten
   - 1.2 Besonderheiten der mobilen Softwareentwicklung
   - 1.3 Einteilung von mobilen Geräten
   - 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 Emulatortest
3.3 App-Deployment

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 Grafisches Design

5. Interaktion zwischen Anwendungskomponenten
   5.1 Intents
   5.2 Services
   5.3 Broadcast Receiver

6. Fortgeschrittene Techniken
   6.1 Threading
   6.2 Anwendungsspeicher

Literatur

Pflichtliteratur

Weiterführende Literatur

- Allen, G. (2021). Android for absolute beginners: Getting started with mobile apps development using the Android Java SDK. Apress.
- Hagos, T. (2020): Learn Android Studio 4: Efficient Java-Based Android Apps Development. Berkeley, CA: Apress.
- Meike, B. G., & Schiefer, L. (2022). Inside the Android OS: Building, customizing, managing, and operating Android system services. Pearson.
- Android Open Source Project (2022). Guide to app architecture. (Available on the Internet).

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Musterklausur
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Projekt: Mobile Software Engineering

Kurscode: DLBCSEMSE02_D

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

Beschreibung des Kurses

Unter Anwendung der erworbenen Kenntnisse, erstellen die Studierenden selbstständig eine mobile Anwendung und dokumentieren deren Konzeption und Umsetzung.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbständig einen Prototyp einer kleinen mobilen Anwendung zur Lösung eines bestimmten Problems zu entwerfen und zu erstellen.
- typische Probleme und Herausforderungen bei der praktischen Umsetzung von kleinen mobilen Anwendungen zu erkennen.
- die Konzeption und Umsetzung kleiner, eigenständig implementierter mobiler Anwendungen zu dokumentieren.

Kursinhalt

- Konzeption, Umsetzung und Dokumentation von kleinen, mobilen Anwendungen anhand einer konkreten Aufgabenstellung.
  Mögliche Themen sind z.B.:
  - Eine Radio-App zur Verbesserung des Austauschs zwischen Hörern und Sendern im Allgemeinen und vor allem zwischen Hörern und Radiomoderatoren im Speziellen.
  - Eine App, die es einer Gruppe von Brettspielfans ermöglicht, ihre regelmäßigen Spielabende besser zu organisieren.
  - Eine App, mit der die Betreuenden von Abschlussarbeiten an der IU ihre Betreuungsprozesse verbessern können.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Guo, L. (2022). The first line of code: Android programming with Kotlin. Springer. ▪ Hagos, T. (2019). Android Studio IDE quick reference: A pocket guide to Android Studio development. Apress. ▪ Vollmer, G. (2017). Mobile App Engineering: Eine systematische Einführung - von den Requirements zum Go Live. dpunkt.verlag.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat myStudium

Studienform	**Kursart**
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Apple Mobile Solution Development

Modulcode: DLAMSD

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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. Holger Klus (Apple Mobile Solution Development I) / Prof. Dr. Holger Klus (Apple Mobile Solution Development II)

Kurse im Modul

- Apple Mobile Solution Development I (DLAMSD01)
- Apple Mobile Solution Development II (DLAMSD02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Apple Mobile Solution Development I • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht Apple Mobile Solution Development II • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht
Anteil der Modulnote an der Gesamtnote s. Curriculum	

Lehrinhalt des Moduls

Apple Mobile Solution Development I

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.

Apple Mobile Solution Development II

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.

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 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.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Bachelor-Programme im Bereich IT & Technik

Apple Mobile Solution Development I

Kurscode: DLAMSD01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Folien	☑ Prüfungsleitfaden

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Folien	☑ Prüfungsleitfaden

Apple Mobile Solution Development II

Kurscode: DLAMSD02

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Folien	☑ Prüfungsleitfaden

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Folien	☑ Prüfungsleitfaden

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Microsoft ERP- Dynamics 365 Business Central - Functional Consultant

Module Code: DLBMSERP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		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

Dr. Aditya Mushyam (Project: Dynamics 365 Business Central - Financial Company Setup) / Dr. Aditya Mushyam (Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution)

Contributing Courses to Module

- Project: Dynamics 365 Business Central - Financial Company Setup (DLBMSERP01)
- Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution (DLBMSERP02)

Module Exam Type

Module Exam	Split Exam Project: Dynamics 365 Business Central - Financial Company Setup • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report • Study Format "Duales myStudium": Written Assessment: Project Report
Weight of Module see curriculum	

Module Contents

Project: Dynamics 365 Business Central - Financial Company Setup

This module empowers students to configure and perform core business processes of a small or medium-sized company in an enterprise resource planning (ERP) system using Microsoft Dynamics 365 Business Central. Therefore, the module will address the core financial setup as well as sales and distribution processes for a small or medium-sized company.

Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution

This module empowers students to configure and perform core business processes of a small or medium-sized company in an enterprise resource planning (ERP) system using Microsoft Dynamics 365 Business Central. Therefore, the module will address the core financial setup as well as sales and distribution processes for a small or medium-sized company.

Learning Outcomes

Project: Dynamics 365 Business Central - Financial Company Setup

On successful completion, students will be able to

- describe the core feature of Business Central as an ERP system for small or medium-sized company.
- initially setup Business Central (SaaS).
- configure a new small or medium-sized demo company in Business Central.
- manage core security settings in Business Central.
- configure financials by setting up the finance module in Business Central.
- configure the chart of accounts in Business Central.

Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution

On successful completion, students will be able to

- configure sales module in Business Central.
- configure purchasing module in Business Central.
- set up inventory management in Business Central.
- configure master data for sales and purchasing in Business Central.
- describe how to perform Business Central operations including selling and purchasing.
- process financial documents.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Project: Dynamics 365 Business Central - Financial Company Setup

Course Code: DLBMSERP01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course aims to empower students to perform financial business processes of a small or medium-sized company using the well-established cloud-based ERP system Microsoft Dynamics 365 Business Central (BC). At first, you will gain important insights into the typical structure of BC. Based on that knowledge, you will be guided to setup a SaaS environment for a demo company in BC. To ensure a safe operation of BC in the cloud you will learn how to configure essential security settings. Next, you will familiarize yourself with the most important and common financial business processes for a small or medium-sized business. Finally, you will configure the accounting module for your demo company in BC.

Course Outcomes

On successful completion, students will be able to

- describe the core feature of Business Central as an ERP system for small or medium-sized company.
- initially setup Business Central (SaaS).
- configure a new small or medium-sized demo company in Business Central.
- manage core security settings in Business Central.
- configure financials by setting up the finance module in Business Central.
- configure the chart of accounts in Business Central.

Contents

- Embarking on the journey of utilizing BC involves a series of pivotal steps. It commences with the fundamental task of setting up the platform itself. This encompasses the creation and meticulous configuration of a company, including the setup of security settings to ensure a secure operational environment. The process further extends to establishing the core functionality, which serves as the backbone of operations. The inclusion of dimensions adds an additional layer of precision to data handling. A critical aspect of the BC framework lies in managing approvals seamlessly through the implementation of workflows, streamlining processes and enhancing efficiency. Within the finance module, a thorough configuration is undertaken. This involves the setup of financial management procedures, which ensures the financial aspect of operations is well-structured and organized. Part of this process includes the establishment of the chart of accounts, providing a foundation for accurate

financial tracking. Moreover, the setup of posting groups refines the financial recording process, facilitating precise categorization. The establishment of journals and bank accounts enhances financial transparency, offering a clear overview of monetary transactions. Notably, payable accounts are configured, ensuring seamless management of outgoing payments. Similarly, the setup of receivable accounts streamlines the handling of incoming payments. Collectively, these steps form a comprehensive roadmap to unleash the full potential of BC, enabling efficient operations and meticulous financial management.

Literature

Compulsory Reading

Further Reading

- Gayer, M., Hauptmann, C., & Ebert, J. (2020). Microsoft Dynamics 365 Business Central: Das Anwenderbuch zur Abwicklung von Geschäftsprozessen (11. Ausgabe). Carl Hanser Verlag.
- Ferner, C. (2020): Microsoft Dynamics 365 Business Central Basiswissen (Auflage 1). BoD – Books on Demand.
- Merk, J. (2020). Microsoft Dynamics 365 BC Finanzbuchhaltung. NEW ERA Publications
- Microsoft Corporation. (2023). Learning path for certification: Dynamics 365 Business Central Functional Consultant.

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Project: Dynamics 365 Business Central - Business Processes with Focus on Sales and Distribution

Course Code: DLBMSERP02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBMSERP01

Course Description

This course aims to empower students to perform sales and distribution processes using the well-established cloud-based ERP system Microsoft Dynamics 365 Business Central (BC). At first, you will gain important insights into the configuration of the sales module for a small or medium-sized company. Based on that knowledge, you will be guided to setup the purchasing module and inventory management in BC. Next, you will familiarize yourself with the configuration of the corresponding master data management. Finally, you will perform common business transaction in the sales and distribution module as well as process core financial documents for your demo company in BC.

Course Outcomes

On successful completion, students will be able to

- configure sales module in Business Central.
- configure purchasing module in Business Central.
- set up inventory management in Business Central.
- configure master data for sales and purchasing in Business Central.
- describe how to perform Business Central operations including selling and purchasing.
- process financial documents.

Contents

- To ensure the smooth flow of business processes in BC, various steps are necessary. First, the configuration of the sales and purchases modules takes place to establish the foundation for efficient work. During this phase, inventory management is set up to ensure an organized inventory flow. An essential step is configuring master data for sales and purchasing, as these form the basis for all subsequent activities. Prices and discounts are also established to create a clear pricing structure. Following this, common operations are performed in Business Central, encompassing both basic tasks and frequent operations. The processing of purchases as well as the handling of sales transactions is a central part of the process and a common operation in BC. Financial documents are processed as well to accurately represent the accounting aspect. Another step involves processing payments and journal entries to meticulously manage the financial aspects. All of these steps contribute to the seamless execution of business activities while maintaining financial integrity.

Literature
Compulsory Reading
Further Reading ▪ Gayer, M., Hauptmann, C., & Ebert, J. (2020). Microsoft Dynamics 365 Business Central: Das Anwenderbuch zur Abwicklung von Geschäftsprozessen (11. Ausgabe). Carl Hanser Verlag. ▪ Ferner, C. (2020): Microsoft Dynamics 365 Business Central Basiswissen (Auflage 1). BoD – Books on Demand. ▪ Microsoft Corporation. (2023). Learning path for certification: Dynamics 365 Business Central Functional Consultant.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

SAP - SAP S/4HANA Business Process Integration - Application Associate

Module Code: DLBSAPBPI

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Knut Linke (Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management) / Prof. Dr. Knut Linke (Project: SAP S/4HANA - Business Processes)

Contributing Courses to Module

- Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management (DLBSAPBPI01)
- Project: SAP S/4HANA - Business Processes (DLBSAPBPI02)

Module Exam Type

Module Exam	Split Exam
	Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management • Study Format "Duales myStudium": Written Assessment: Project Report • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report Project: SAP S/4HANA - Business Processes • Study Format "Distance Learning": Written Assessment: Project Report • Study Format "myStudies": Written Assessment: Project Report • Study Format "Duales myStudium": Written Assessment: Project Report
Weight of Module see curriculum	

Module Contents

Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management

This module empowers students to configure and perform core business processes of medium-sized and large companies in an enterprise resource planning (ERP) system using SAP S/4HANA and the user interface SAP Fiori. The module consists of two steps, each catering to specific facets. In the first step, attention is directed towards the core financial setup as well as the preliminary configuration of the Human Capital Management module using a demo company as an illustration. This step lays down a robust foundation in these domains. Moving on to the second step, the focus shifts to expanding the initial setup by integrating business processes related to sales, distribution, and production.

Project: SAP S/4HANA - Business Processes

Learning Outcomes

Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management

On successful completion, students will be able to

- navigate confidently within the SAP S/4HANA ERP system.
- explain the organizational structures.
- understand the concept of master data.
- explain financial accounting (FI) module.
- explain management accounting (CO) module.
- explain the employee master data record (HCM).

Project: SAP S/4HANA - Business Processes

On successful completion, students will be able to

- describe the source to pay business process (MM).
- describe warehouse management systems (WM).
- explain the design to operate business process (PP).
- describe the order to cash business process (SD).
- create a project structure (PS).
- defining the organizational levels used in enterprise asset management (EAM).

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology fields

Project: SAP S/4HANA - Financial Company Setup incl. Human Capital Management

Course Code: DLBSAPBPI01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course aims to empower students to perform financial business processes of medium-sized and large companies using the well-established ERP system SAP S/4HANA (S4H). At first, you will gain important insights into the typical organizational structure and navigation within S4H. You will understand the new user experience concept of SAP Fiori. Based on that knowledge, you will get in contact with the concept of master data in S4H. Next, you will familiarize yourself with the most important and common financial business processes in the financial accounting (FI) and management accounting (CO) module of S4H. Finally, you will configure the employee master data record in the Human Capital Management (HCM) module of S4H.

Course Outcomes

On successful completion, students will be able to

- navigate confidently within the SAP S/4HANA ERP system.
- explain the organizational structures.
- understand the concept of master data.
- explain financial accounting (FI) module.
- explain management accounting (CO) module.
- explain the employee master data record (HCM).

Contents

- The course provides a comprehensive introduction into SAP S/4HANA starting with the overall SAP S/4HANA Enterprise Management: Overview. Therefore, the course offers a comprehensive and presentation of various key concepts and functions relevant in the world of SAP S/4HANA. Furthermore, it focuses on the new user experience brought by SAP Fiori UX. The course covers the basics of SAP S/4HANA as well as the various organizational structures that exist within this system. A central concept addressed is that of master data. The subjects of Financial Accounting and Management Accounting (Record-to-Report processing) are thoroughly examined, providing an overview. Within these areas, Financial Accounting (FI) is explained, and Management Accounting (CO) is illuminated further. The integration between FI and CO is also outlined. The fundamentals of Financial Accounting and Management Accounting (Record-to-Report processing) are further delved into. This includes the definitions of General Ledger (G/L) accounts and cost elements, as well as

the definition of cost centers. Step-by-step instructions for posting G/L account documents and handling business partners and invoices are conveyed. The management of Asset Accounting, Activity Types, and Internal Orders is also comprehensively explained. The course also addresses the realm of Human Capital Management (HCM). This covers organizational management in HCM, as well as the significance of HCM master data. Another important aspect is the integration with SAP Success Factors.

Literature

Compulsory Reading

Further Reading

- Fitzner, W., Fitzner, D. (2021). SAP S/4HANA: Der Grundkurs für Einsteiger und Anwender. SAP Press
- Fix, W., Plota, R. (2021). SAP – Der technische Einstieg: Der Standardtitel für Ausbildung, Studium und Quereinstieg. SAP Press
- SAP SE. (2023). SAP Learning journey "Explore Integrated Business Processes in SAP S/4HANA".
- SAP SE. (2023). SAP Learning journey "Discovering End-to-End Business Processes for the Intelligent Enterprise".

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Project: SAP S/4HANA - Business Processes

Course Code: DLBSAPBPI02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBSAPBPI01

Course Description

This course aims to empower students to perform sales and distribution processes of medium-sized and large companies using the well-established ERP system SAP S/4HANA (S4H).At first, you will gain important insights into the configuration of the purchasing (MM) and warehouse management (WM) modulewithin S4H. You willalso understand the production process (PP) of S4H. Based on that knowledge, you willget in contact with the lead to cash business process (SD) in S4H. Next, you will familiarize yourself with the project system (PS) in S4H while creating project steps and structures. Finally, you will defining the organizational levels and for the management and maintenance of the company's physical assets in the enterprise asset management (EAM) module of S4H.

Course Outcomes

On successful completion, students will be able to

- describe the source to pay business process (MM).
- describe warehouse management systems (WM).
- explain the design to operate business process (PP).
- describe the order to cash business process (SD).
- create a project structure (PS).
- defining the organizational levels used in enterprise asset management (EAM).

Contents

- The course covers a wide range of processes and concepts within SAP S/4HANA: Purchase to Pay Processing in SAP S/4HANA: Exploring the Purchase to Pay business process, including the definition of master data involved. This encompasses creating vendor master records, listing vendor-specific master data records, generating purchase requisitions, crafting purchase orders, posting goods receipts for purchase orders, and managing vendor invoices. The automatic payment run process is also elucidated. Warehouse Management - Stock Transfer: This section delves into Warehouse Management (WM) structures and usage, highlighting the distinctions between Extended Warehouse Management (EWM), WM, and Inventory Management (IM). The process of handling stock transfer orders is outlined. Plan to Produce Business Process in SAP S/4HANA: Understanding the Plan to Produce process within SAP S/4HANA, which encompasses defining master data, creating product cost estimates, planning product demand through integrated planning, establishing Material Requirements Planning (MRP) processes, and executing advanced planning. Advanced

Planning - Describing the Manufacturing Business Process: Exploring the manufacturing business process, starting from the creation and release of production orders to material withdrawal, order confirmation, materials goods receipt, and period-end closing activities. Order to Cash Processing in SAP S/4HANA: This section focuses on the Order to Cash business process, describing the master data used in sales and distribution. The process involves creating customer master records, setting up condition records, processing sales orders, managing delivery documents, generating customer invoices, and handling related activities. Project System (PS): Detailing the steps within Project System, including creating project structures, project planning, budgeting, project execution, and concluding with period-end closing activities. SAP Enterprise Asset Management (EAM): Covering the business steps in SAP EAM, describing the master data utilized, creating notifications, processing maintenance orders, executing maintenance tasks, and wrapping up with period-end closing activities.

Literature

Compulsory Reading

Further Reading

- Fitzner, W., Fitzner, D. (2021). SAP S/4HANA: Der Grundkurs für Einsteiger und Anwender. SAP Press
- Fix, W., Plota, R. (2021). SAP – Der technische Einstieg: Der Standardtitel für Ausbildung, Studium und Quereinstieg. SAP Press
- SAP SE. (2023). SAP Learning journey “Explore Integrated Business Processes in SAP S/4HANA”.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Karriere-Entwicklung

Modulcode: DLBKAENT

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum		BA	10	300 h

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

Modulverantwortliche(r)

Prof. Dr. Heike Schiebeck (Persönlicher Karriereplan) / Prof. Dr. Heike Schiebeck (Persönlicher Elevator Pitch)

Kurse im Modul

- Persönlicher Karriereplan (DLBKAENT01)
- Persönlicher Elevator Pitch (DLBKAENT02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Persönlicher Karriereplan • Studienformat "Fernstudium": Advanced Workbook (100%) • Studienformat "myStudium": Advanced Workbook • Studienformat "Duales myStudium": Advanced Workbook Persönlicher Elevator Pitch • Studienformat "Fernstudium": Konzeptpräsentation (100%) • Studienformat "Duales myStudium": Konzeptpräsentation (100) • Studienformat "myStudium": Konzeptpräsentation

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Persönlicher Karriereplan

- Karrieretheorien und -modelle
- Berufliche Entwicklung
- Auswahl möglicher Karrieren
- Personal Branding
- Karrierestrategie
- Globale Karrieren
- Stellensuche

Persönlicher Elevator Pitch

Durch die Anwendung von Selbstreflexion, Selbstwahrnehmung auf der Basis relevanter beruflicher Erfolgsparameter sollen die Studierenden Karriereziele, Karriereschritte und ihre Karrierestrategie entwickeln. Unter Berücksichtigung ihrer aktuellen beruflichen und/oder Studiensituation werden die zentralen Elemente einer kurz- und mittelfristigen Karriereplanung von den Studierenden für ihre individuelle Situation erarbeitet. Am Ende des Kurses sind die Studierenden in der Lage, ihren persönlichen Elevator Pitch zu präsentieren und zielgruppen- bzw. publikumsgerecht zu kommunizieren. Auf diese Weise reflektieren sie ihre aktuelle berufliche Situation. Der persönliche Elevator Pitch ist das Herzstück des Personal Branding und unterstützt die Vermittlung dieser Vision bei persönlichen Netzwerkaktivitäten.

Qualifikationsziele des Moduls

Persönlicher Karriereplan

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- dargestellte Karrieretheorien und -modelle im Hinblick auf ihre persönliche Situation zu verstehen, anzuwenden und zu reflektieren, um zu einem Konzept bzw. Bild einer gewünschten Karriere zu gelangen.
- das Konzept der Karriere- und Laufbahnplanung zu verstehen und kritisch zu reflektieren.
- die Bedeutung einer strategisch orientierten Karriereplanung zu verstehen.
- die Bedeutung einer persönlichen Standortbestimmung zu verstehen und durchzuführen, um die eigene Persönlichkeit und Motivation herauszuarbeiten und die eigenen Werte, Stärken, Kompetenzen, Fähigkeiten und Interessen zu ermitteln.
- die Notwendigkeit des Aufbaus und der Pflege der eigenen persönlichen Marke zu verstehen.
- die unterschiedlichen Prozesse der Stellensuche in nationalen/internationalen Kontexten zu verstehen und dementsprechend kontextabhängige Bewerbungen zu erstellen.
- die Prinzipien globaler Karrieren zu verstehen und zu wissen, wie sie im internationalen Umfeld agieren können.

Persönlicher Elevator Pitch

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihre Karriereziele, Karriereschritte und den persönlichen Status Quo auf Basis ihrer bisherigen Leistungen zu ermitteln.
- ihre aktuelle Situation zu reflektieren und zu definieren, wohin sie sich entwickeln wollen und welchen Karriereschritt sie anstreben.
- eine Karrierestrategie zu entwickeln, indem sie persönliche Karriereziele und einen kohärenten Aktionsplan erstellen.
- den Prozess des Aufbaus einer persönlichen Marke zu verstehen und anzuwenden.
- ihre Identität, ihre Fähigkeiten, ihre Profession, die Gründe für ihre Überzeugung und die notwendigen "Investitionen" zur Erreichung der Karriereschritte zu definieren.
- ihre persönlichen Stärken und ihren wichtigsten Antrieb zu identifizieren.
- die Macht der effektiven Kommunikation, des Netzwerkens und des Storytellings zu verstehen.
- die Prinzipien und den Prozess der Gestaltung eines starken persönlichen Elevator Pitchs zu verstehen und anzuwenden.
- ihren persönlichen Elevator Pitch kritisch zu reflektieren und an die Besonderheiten des Kontexts, des Publikums, der Zielgruppe und der Art der Präsentation anzupassen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der Hochschule**
Baut auf Modulen aus dem Bereich Human Resources auf	Alle Bachelor-Programme im Bereich Human Resources

Persönlicher Karriereplan

Kurscode: DLBKAENT01

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

Beschreibung des Kurses

In der heutigen komplexen und sich ständig wandelnden Umwelt variieren die Formen von Karrieren je nach Kontext, Werteverständnis und Marktdynamik. Die "klassische Karriereleiter", die man erklimmt und die die einzige vorherrschende Form der Karriere war, ist längst überholt, und der:die Einzelne wird mit einer Vielzahl von Möglichkeiten in Bezug auf die Branche oder die Arbeitsplatzwahl und die Arbeitsgestaltung konfrontiert. Es ist wichtiger denn je, die große Vielfalt an beruflichen Optionen zu berücksichtigen, insbesondere für gut ausgebildete Personen, um fundierte Entscheidungen zu treffen. Dieser Kurs soll die Studierenden dabei unterstützen, sich durch diese Komplexität ihrer persönlichen Karriereplanung zu manövrieren, wobei Selbsterkenntnis, Selbstreflexion und Zielsetzung wichtige Elemente dieses Prozesses sind. Geleitet von zentralen Elementen der Karrieretheorie, Karrieremodellen und Forschungsergebnissen werden den Studierenden Instrumente und Reflexionsübungen an die Hand gegeben, um zu einer soliden, direkt anwendbaren Strategie zu gelanden, mit der sie ihre beruflichen Fortschritte und Karriereschritte weiter vorantreiben können.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- dargestellte Karrieretheorien und -modelle im Hinblick auf ihre persönliche Situation zu verstehen, anzuwenden und zu reflektieren, um zu einem Konzept bzw. Bild einer gewünschten Karriere zu gelangen.
- das Konzept der Karriere- und Laufbahnplanung zu verstehen und kritisch zu reflektieren.
- die Bedeutung einer strategisch orientierten Karriereplanung zu verstehen.
- die Bedeutung einer persönlichen Standortbestimmung zu verstehen und durchzuführen, um die eigene Persönlichkeit und Motivation herauszuarbeiten und die eigenen Werte, Stärken, Kompetenzen, Fähigkeiten und Interessen zu ermitteln.
- die Notwendigkeit des Aufbaus und der Pflege der eigenen persönlichen Marke zu verstehen.
- die unterschiedlichen Prozesse der Stellensuche in nationalen/internationalen Kontexten zu verstehen und dementsprechend kontextabhängige Bewerbungen zu erstellen.
- die Prinzipien globaler Karrieren zu verstehen und zu wissen, wie sie im internationalen Umfeld agieren können.

Kursinhalt

1. Karrieretheorien und -ansätze
    1.1 Definition und Einordnung von Karriere

- 1.2 Traditionelle Karriertheorien und -modelle
- 1.3 Neue Karrieremodelle und -theorien
- 1.4 Karrierelernzyklus

2. Karriereentwicklung
   - 2.1 Karrieremotive
   - 2.2 Karriererollen
   - 2.3 Karriereleistung

3. Karriereplanung
   - 3.1 Grundlagen der Karriereplanung
   - 3.2 Prozess der Karriereplanung
   - 3.3 Unwägbarkeiten der Karriereplanung

4. Individuelle Beschreibung
   - 4.1 Persönlichkeit
   - 4.2 Werte
   - 4.3 Kompetenzen, Fähigkeiten, Stärken und Interessensfelder

5. Karrieremöglichkeiten
   - 5.1 Mögliche Karrierepfade
   - 5.2 Karriereformen
   - 5.3 Beschäftigungsfähigkeit
   - 5.4 Berufliche Identität

6. Entwicklung einer Karrierestrategie und Management der Karriere
   - 6.1 Karrierekapital
   - 6.2 Karriereziele
   - 6.3 Karriereerfolg
   - 6.4 Selbstreflexion
   - 6.5 Personal Branding

7. Globale Karrieren
   - 7.1 Globale Karriereformen
   - 7.2 Individuelle Eigenschaften globaler Führungskräfte
   - 7.3 Rolle der Interkulturalität
   - 7.4 Diversität und Inklusion

8. Arbeitssuche in Deutschland und im Ausland

8.1 Datenbanken für die Arbeitssuche
8.2 Netzwerke und Plattformen
8.3 Gestaltung von Lebenslauf und Anschreiben
8.4 Schriftliche Bewerbung und Video-Bewerbung
8.5 Auswahlverfahren

Literatur

Pflichtliteratur

Weiterführende Literatur

- Butto Zarzar, C., & Klein, W. K. (2020). Beruflich vorankommen mit dem 5-Punkte-Plan. Haufe Taschenguide.
- Ibarra, H. (2004). Working Identity: Unconventional Strategies for Reinventing Your Career. Harvard Business School Press.
- Kauffeld, S., & Spurk, D. (2018). Handbuch Karriere und Laufbahnmanagement. Springer.
- Ng, T. W. H., Eby, L. T., Sorensen, K. L., & Feldman, D. C. (2005). Predictors of objective and subjective career success: A meta-analysis. Personnel psychology, 58(2), 367-408.
- Ng, T. W. H., & Feldman, D. C. (2014). Subjective career success: A meta-analytic review. Journal of Vocational Behavior, 85(2), 169-179.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
	☑ Audio	
☑ Recorded Live Sessions	☑ Folien	

Studienformat myStudium

Studienform	Kursart
myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Skript
- ☑ Video
- ☑ Audio
- ☑ Folien

Prüfungsvorbereitung
- ☑ Online Tests
- ☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Theoriekurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Ja
Prüfungsleistung	Advanced Workbook

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed	☑ Skript	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Prüfungsleitfaden
☑ Recorded Live Sessions	☑ Audio	
	☑ Folien	

Persönlicher Elevator Pitch

Kurscode: DLBKAENT02

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
BA	Deutsch		5	DLBKAENT01

Beschreibung des Kurses

Die Karriereformen variieren je nach Kontext oder persönlichen Vorlieben in der sich ständig verändernden, anspruchsvollen und komplexen Umwelt von heute. Veränderungen im Umfeld, wie z.B. im Bereich der Technologie, Nachhaltigkeit oder dem Aufkommen künstlicher Intelligenz, zwingen den:die Einzelne:n dazu, berufliche Übergange selbst in die Hand zu nehmen. Persönliche Bemühungen, die eigene Karriere weiterzuentwickeln, etwa durch die Akquisition neuer Projekte, Jobs oder Arbeitgeber:innen, erfordern die richtigen Strategien, um erfolgreich zu sein. Kontakte durch gezieltes Netzwerken aufzubauen und zu pflegen sowie die Entwicklung der eigenen Marke spielen dabei eine besondere Rolle. Gerade für Berufseinsteiger:innen nach abgeschlossener Ausbildung/Studium ist effektives Netzwerken der Schlüssel für den Berufseinstieg und die Karriereentwicklung in diesen turbulenten Zeiten. Darüber hinaus ist Personal Branding ein Konzept, das nicht nur in der Forschung an Relevanz gewonnen hat, sondern auch in der Karriereberatung breite Anwendung findet. Die Entwicklung und Vermittlung einer persönlichen Marke ist ein zentrales Thema dieses Kurses. Durch den Einsatz des Personal Branding-Ansatzes bei Netzwerk-Aktivitäten kann der:die Einzelne zu seinem:ihrem beruflichen Erfolg beitragen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihre Karriereziele, Karriereschritte und den persönlichen Status Quo auf Basis ihrer bisherigen Leistungen zu ermitteln.
- ihre aktuelle Situation zu reflektieren und zu definieren, wohin sie sich entwickeln wollen und welchen Karriereschritt sie anstreben.
- eine Karrierestrategie zu entwickeln, indem sie persönliche Karriereziele und einen kohärenten Aktionsplan erstellen.
- den Prozess des Aufbaus einer persönlichen Marke zu verstehen und anzuwenden.
- ihre Identität, ihre Fähigkeiten, ihre Profession, die Gründe für ihre Überzeugung und die notwendigen "Investitionen" zur Erreichung der Karriereschritte zu definieren.
- ihre persönlichen Stärken und ihren wichtigsten Antrieb zu identifizieren.
- die Macht der effektiven Kommunikation, des Netzwerkens und des Storytellings zu verstehen.
- die Prinzipien und den Prozess der Gestaltung eines starken persönlichen Elevator Pitchs zu verstehen und anzuwenden.
- ihren persönlichen Elevator Pitch kritisch zu reflektieren und an die Besonderheiten des Kontexts, des Publikums, der Zielgruppe und der Art der Präsentation anzupassen.

Kursinhalt

- Das Kernelement dieses Kurses ist ein persönlicher Elevator Pitch mithilfe eines Personal Branding-Canvas. Die Entwicklung einer persönlichen Marke ist nicht nur für Freiberufler:innen oder Unternehmer:innen relevant, sondern auch für Personen, die ihre eigene Weiterentwicklung auf der Karriereleiter innerhalb ihrer Organisation anstreben, oder für diejenigen, die einen Arbeitsplatz suchen. Nachdem die Teilnehmer:innen die Merkmale und Hintergründe des Personal Branding und den zugrundeliegenden Prozess verstanden haben, werden sie in der Lage sein, diesen Prozess auf ihre eigene Person und Situation anzuwenden.
- Selbstwahrnehmung ist die wichtigste "Zutat" für den Aufbau einer wirksamen persönlichen Marke ist, werden die Teilnehmer:innen dazu ermutigt, sich auf eine intensive Reise der Selbstreflexion zu begeben, um ihr Verständnis für ihre Identität, ihre Fähigkeiten, ihren Beruf und ihre Gründe für eine persönliche Marke zu vertiefen und in der Folge einen persönlichen Elevator Pitch zu entwickeln.
- Der Elevator Pitch ist das Herzstück und die Essenz des Personal Branding und ermöglicht es dem:der Einzelnen, sich wichtigen Personen und potenziellen Arbeitgeber:innen kurz und prägnant zu präsentieren. Nachdem die Studierenden die Prinzipien und Erfolgsfaktoren eines Elevator Pitch verstanden haben, können sie ihren eigenen Elevator Pitch entwickeln. Sie werden lernen, Aspekte wie Timing, Nutzen, klare Positionierung und das Zielpublikum durch eine mündliche Form der Präsentation entsprechend zu berücksichtigen. Darüber hinaus wird die Rolle von Kommunikations-, Netzwerk- und Storytelling-Prinzipien hervorgehoben.
- Kenntnis der Kernelemente und Erfolgsfaktoren des persönlichen Elevator Pitch im Rahmen der individuellen Karriereentwicklung.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Dowling, D. (2009). How to Perfect an Elevator Pitch About Yourself. Harvard Business Review. https://hbr.org/2009/05/how-to-perfect-an-elevator-pit.
- Gorbatov, S., Khapova, S. N., & Lysova, E. I. (2018). Personal branding: Interdisciplinary systematic review and research agenda. Frontiers in psychology, 2238.
- Gorbatov, S., Khapova, S. N., & Lysova, E. I. (2019). Get noticed to get ahead: The impact of personal branding on career success. Frontiers in psychology, 2662.
- Spall, C., & Schmidt, H. J. (2019). Personal Branding. Was Menschen zu starken Marken macht. Springer Gabler.
- Woodside, A. G. (2010). Brand consumer storytelling theory and research: Introduction to a Psychology & Marketing special issue. Psychology & Marketing, 27(6), 531-540.
- Zayats, M. (2020). Digital Personal Branding. Über den Mut, sichtbar zu sein. Ein Guide für Menschen und Unternehmen. Springer Gabler.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Konzeptpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Konzeptpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden		
Tutorielle Betreuung	**Lernmaterial**	**Prüfungsvorbereitung**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Folien	☑ Prüfungsleitfaden

Studienformat myStudium

Studienform	Kursart
myStudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Konzeptpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden

Tutorielle Betreuung
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Lernmaterial
- ☑ Folien

Prüfungsvorbereitung
- ☑ Prüfungsleitfaden

AWS Cloud Specialization

Module Code: DLBAWSCLSP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	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

Georgi Dimchev (Project: AWS - Cloud Essentials) / Prof. Dr. Tianxiang Lu (Project: AWS - Cloud Advanced)

Contributing Courses to Module

- Project: AWS - Cloud Essentials (DLBPAWSCLES01)
- Project: AWS - Cloud Advanced (DLBPAWSCLAD01)

Module Exam Type

Module Exam

Split Exam

Project: AWS - Cloud Essentials

- Study Format "myStudies": Written Assessment: Project Report
- Study Format "Duales myStudium": Written Assessment: Project Report
- Study Format "Distance Learning": Written Assessment: Project Report

Project: AWS - Cloud Advanced

- Study Format "Distance Learning": Written Assessment: Project Report
- Study Format "Duales myStudium": Written Assessment: Project Report
- Study Format "myStudies": Written Assessment: Project Report

Weight of Module
see curriculum

Module Contents

Project: AWS - Cloud Essentials

Students will learn the foundational concepts and services of Amazon Web Services (AWS), covering its core infrastructure services including computing, storage, and networking through practical experience. Emphasis is placed on practical skills for deploying Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions.

Project: AWS - Cloud Advanced

This course offers advanced understanding of AWS, with a particular emphasis on specialized areas such as Solutions Architecture, Compliance & Security, and AI & Machine Learning. Students will acquire hands-on expertise in these areas, with the goal of enabling them to deploy laaS, Paas, or SaaS workloads using AWS, effectively tackle real-life interdisciplinary challenges, and confidently handle service configurations within the AWS cloud console.

Learning Outcomes

Project: AWS - Cloud Essentials

On successful completion, students will be able to

- understand the core services of AWS including compute, network, databases, and storage, deployment models (on-premises, hybrid, and vpc).
- explain the shared responsibility model, describe the basic global infrastructure and core security services.
- describe the AWS Well-Architected Framework and the basics of AWS Cloud Migration.
- get familiar with the terminology and concepts related to AWS Services, the AWS Management Console, AWS security measures, IAM and AWS networking services.
- apply and manage core service settings within the AWS cloud console effectively.
- assess data storage services in AWS to meet various application needs.
- plan and implement a scenario-based serverless service for small or medium-sized companies.
- configure basic network security using Amazon CloudWatch monitoring features for simple use cases in AWS, ensuring secure cloud operations.
- critically examine the core billing, account management, and pricing models and explain how to use pricing tools to make cost-effective choices for AWS services.

Project: AWS - Cloud Advanced

On successful completion, students will be able to

- understand and articulate the core services provided by AWS within chosen specialization tracks, including Solutions Architect, Compliance & Security, and AI & Machine Learning.
- critically examine the pros and cons of developing and deploying real-world scenarios using AWS IaaS, PaaS, vs. SaaS and public, private or hybrid deployment demonstrating a clear grasp of the necessary service and deployment intricacies.
- manage and configure profound service settings within the AWS cloud console, showing depth in technical proficiency and operational capabilities.
- critically assess, test and monitor the effect of different AWS deployment features, addressing interdisciplinary challenges through the appropriate use of AWS cloud services in realistic use cases.
- assess and critically reflect on AWS-based solutions, considering industry compliance and security requirements, ensuring a robust understanding of the legal and regulatory framework.
- apply and implement machine learning and artificial intelligence concepts using AWS to solve real-world problems, demonstrating innovative thinking and practical application of theoretical knowledge.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Bachelor Programs in the IT & Technology field

Project: AWS - Cloud Essentials

Course Code: DLBPAWSCLES01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Amazon Web Services (AWS) is a comprehensive cloud computing platform provided by Amazon that offers scalable computing power, storage, and various other functionalities to help businesses and individuals deploy applications and manage data efficiently. It reduces the need for physical hardware, thus lowering costs and increasing flexibility by allowing users to access services and resources on-demand from anywhere in the world. This service is highly relevant for daily life and business as it supports a wide range of applications and services, from hosting websites to supporting IoT devices and big data analytics, ultimately facilitating innovation, scalability, and global operations.This course prepares students for the AWS Cloud Practitioner Certificate, providing a foundational understanding of AWS core services. Students will learn to articulate the benefits and use cases of AWS IaaS, PaaS, and SaaS, and grasp the basics of public, private, and hybrid cloud deployments. The course emphasizes practical skills in managing and configuring AWS services, ensuring students can effectively navigate the AWS cloud console. It lays the groundwork for critical assessments of AWS deployment features, addressing compliance and security requirements, and preparing students for more advanced AWS certifications and applications

Course Outcomes

On successful completion, students will be able to

- understand the core services of AWS including compute, network, databases, and storage, deployment models (on-premises, hybrid, and vpc).
- explain the shared responsibility model, describe the basic global infrastructure and core security services.
- describe the AWS Well-Architected Framework and the basics of AWS Cloud Migration.
- get familiar with the terminology and concepts related to AWS Services, the AWS Management Console, AWS security measures, IAM and AWS networking services.
- apply and manage core service settings within the AWS cloud console effectively.
- assess data storage services in AWS to meet various application needs.
- plan and implement a scenario-based serverless service for small or medium-sized companies.
- configure basic network security using Amazon CloudWatch monitoring features for simple use cases in AWS, ensuring secure cloud operations.
- critically examine the core billing, account management, and pricing models and explain how to use pricing tools to make cost-effective choices for AWS services.

Contents

- This course offers a comprehensive exploration of Amazon Web Services (AWS), focusing on its core services such as computing, networking, databases, and storage solutions. Students will delve into the AWS shared responsibility model, understand the global infrastructure, and learn about the integral security services provided. This also covers the AWS Well-Architected Framework and an introduction of the fundamentals for cloud migration strategies. Through hands-on exercises, students will gain proficiency in managing AWS environments using the AWS Management Console and implement security measures via AWS Identity and Access Management (IAM) and network services. Additionally, the course emphasizes the importance of cost management, enabling students to critically analyze AWS pricing models to make informed financial decisions for cloud-based solutions.

Literature

Compulsory Reading

Further Reading

- AWS Training and Certification Skill Builder. (2024). AWS Cloud Practitioner Essentials (7 hours).
- AWS Training and Certification Skill Builder. (2024). AWS Cloud Quest: Cloud Practitioner.
- AWS Training and Certification Skill Builder. (2024). AWS Technical Essentials (4 hours).
- AWS Training and Certification Skill Builder. (2024). Serverless – Knowledge Badge Readiness Path (13 hours).
- AWS Training and Certification Skill Builder. (2024). Standard Exam Prep Plan: AWS Certified Cloud Practitioner (CLF-C02) (18 hours).

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Slides	☑ Guideline
☑ Intensive Live Sessions/Learning Sprint		
☑ Recorded Live Sessions		

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Project: AWS - Cloud Advanced

Course Code: DLBPAWSCLAD01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

AWS (Amazon Web Services) is a comprehensive cloud computing platform provided by Amazon that offers scalable computing power, storage, and various other functionalities to help businesses and individuals deploy applications and manage data efficiently. It reduces the need for physical hardware, thus lowering costs and increasing flexibility by allowing users to access services and resources on-demand from anywhere in the world. This service is highly relevant for daily life and business as it supports a wide range of applications and services, from hosting websites to supporting IoT devices, big data analytics and machine learning, ultimately facilitating innovation, scalability, and global operations. The course prepares students for the AWS Cloud Solution Architect Professional Certificate. It dives deeper into AWS core services, focusing on sophisticated deployment and management techniques. Students will critically examine and apply real-world scenarios using AWS IaaS, PaaS, and SaaS, and navigate complex deployment models. They will gain technical proficiency in managing advanced service settings within the AWS cloud console and address interdisciplinary challenges through hands-on practice. Additionally, the course covers assessing AWS solutions for compliance and security, ensuring robust understanding of legal frameworks. Students will also implement machine learning and AI concepts to solve real-world problems, fostering innovative thinking and practical application, and preparing them for the dynamic demands of the tech industry.

Course Outcomes

On successful completion, students will be able to

- understand and articulate the core services provided by AWS within chosen specialization tracks, including Solutions Architect, Compliance & Security, and AI & Machine Learning.
- critically examine the pros and cons of developing and deploying real-world scenarios using AWS IaaS, PaaS, vs. SaaS and public, private or hybrid deployment demonstrating a clear grasp of the necessary service and deployment intricacies.
- manage and configure profound service settings within the AWS cloud console, showing depth in technical proficiency and operational capabilities.
- critically assess, test and monitor the effect of different AWS deployment features, addressing interdisciplinary challenges through the appropriate use of AWS cloud services in realistic use cases.
- assess and critically reflect on AWS-based solutions, considering industry compliance and security requirements, ensuring a robust understanding of the legal and regulatory framework.
- apply and implement machine learning and artificial intelligence concepts using AWS to solve real-world problems, demonstrating innovative thinking and practical application of theoretical knowledge.

Contents

- This course ensures students gain a comprehensive understanding of AWS, specializing in Solutions Architect, Compliance & Security, and AI & Machine Learning. They will articulate core AWS services and critically examine the pros and cons of deploying real-world scenarios using AWS IaaS, PaaS, SaaS, and different deployment models (public, private, hybrid).
- Students will manage and configure service settings within the AWS cloud console, demonstrating technical proficiency. They will assess, test, and monitor AWS deployment features, addressing interdisciplinary challenges using realistic use cases. Additionally, students will evaluate AWS-based solutions for industry compliance and security, understanding the legal and regulatory frameworks.
- The course also covers applying machine learning and AI concepts using AWS to solve real-world problems, encouraging innovative thinking and practical application. This approach prepares students to excel in cloud architecture, compliance protocols, security measures, and AI-driven problem-solving, ensuring readiness for the tech industry's dynamic demands.

Literature
Compulsory Reading
Further Reading ▪ AWS Training and Certification Skill Builder. (2024). AWS Solutions Architect – Knowledge Badge Readiness Path (51 hours). ▪ AWS Training and Certification Skill Builder. (2024). Generative AI Learning Plan for Developers (12 hours). ▪ AWS Training and Certification Skill Builder. (2024). Online Course Supplement: Practical Data Science with Amazon SageMaker (1 day).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

AI Prompting Techniques and Process Innovation with Copilot

Module Code: DLBEAIPTPICOP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	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. Knut Linke (Project: AI Excellence with Creative Prompting Techniques) / Aditya Mushyam (Project: Process Innovation with Copilot)

Contributing Courses to Module

- Project: AI Excellence with Creative Prompting Techniques (DLBPKIEKPT01_E)
- Project: Process Innovation with Copilot (DLBPPICOP01)

Module Exam Type

Module Exam	Split Exam
	Project: AI Excellence with Creative Prompting Techniques • Study Format "myStudies": Oral Project Report • Study Format "Duales myStudium": Oral Project Report • Study Format "Distance Learning": Oral Project Report Project: Process Innovation with Copilot • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module
see curriculum

Module Contents

Project: AI Excellence with Creative Prompting Techniques

In this module, the students delve into the world of generative AI applications, creating AI-generated content like text, images, and videos, while learning to use, analyze, and evaluate these systems in their respective study fields.

Project: Process Innovation with Copilot

In this course, students will deepen their understanding and skills in working with Microsoft Copilot, an advanced tool for supporting various work processes through automation, text generation, and data analysis. A special focus will be placed on the ethical and data protection challenges that can arise when using such technologies.

Learning Outcomes

Project: AI Excellence with Creative Prompting Techniques

On successful completion, students will be able to

- comprehend and apply basic prompting techniques in generative AI applications.
- analyze and evaluate the effectiveness of the basic prompts.
- apply ethical considerations to the design and use of AI for basic prompting techniques.
- design, implement, and refine effective prompts to real-world scenarios through hands-on exercises.
- showcase creative and innovative thinking in the application of prompting techniques to solve complex problems in their field of studies.

Project: Process Innovation with Copilot

On successful completion, students will be able to

- understand the basic functions and applications of Microsoft Copilot, including in the fields of text generation and data analysis.
- recognize the possibilities for automating work processes using Copilot and its contribution to efficiency improvement.
- understand interdisciplinary collaboration with Copilot.
- identify and evaluate potential application areas of Copilot in a professional context.
- understand and discuss ethical and data protection aspects of using Copilot.
- develop a critical reflection on the advantages and disadvantages of using Copilot.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology field

Project: AI Excellence with Creative Prompting Techniques

Course Code: DLBPKIEKPT01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, students explore the fascinating world of prompting in generative AI applications. They engage in hands-on exercises to create new AI-generated content including text, images, and videos. Through these exercises, students learn how to effectively use, analyze, and evaluate these systems within their respective fields of study.

Course Outcomes

On successful completion, students will be able to

- comprehend and apply basic prompting techniques in generative AI applications.
- analyze and evaluate the effectiveness of the basic prompts.
- apply ethical considerations to the design and use of AI for basic prompting techniques.
- design, implement, and refine effective prompts to real-world scenarios through hands-on exercises.
- showcase creative and innovative thinking in the application of prompting techniques to solve complex problems in their field of studies.

Contents

- In this course, students work on a basic practical implementation of a generative AI use case by choosing from a selection provided in the complementary guideline. The course provides practical examples as learning materials and exercises with basic prompting techniques for open-source text, image, and video generation use cases. The exercises are designed to inspire and guide students in completing their own generative AI use case work, which includes a use case description, chosen prompting techniques, outcomes, and critical evaluations from both technical and ethical perspectives.

Literature
Compulsory Reading
Further Reading ▪ Dang, H., Mecke, L., Lehmann, F., Goller, S., & Buschek, D. (2022). How to prompt? Opportunities and challenges of zero- and few-shot learning for human-AI interaction in creative applications of generative models. arXiv. https://arxiv.org/pdf/2209.01390.pdf ▪ Eapen, T. T., Finkenstadt, D. J., Folk, J., & Venkataswamy, L. (2023). How generative AI can augment human creativity. Harvard Business Review, July–August, 56–64. ▪ Wei, J., Wang, X., Schuurmans, D., Bosma, M. Ichter, B., Xia, F., Chi, E. H., Le., Q. V., & Zhou, D. (2023). Chain-of-though prompting elicit reasoning in large language models. arXiv. https://arxiv.org/pdf/2201.11903.pdf

Study Format myStudies

Study Format	Course Type
myStudies	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Duales myStudium

Study Format	Course Type
Duales myStudium	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Project: Process Innovation with Copilot

Course Code: DLBPPICOP01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The integration of Artificial Intelligence (AI) into everyday work is revolutionizing how we handle tasks, analyze information, and make decisions. Microsoft Copilot is at the forefront of this development, offering numerous opportunities to enhance efficiency through automation and intelligent data processing.In this course, students explore the diverse functions of Microsoft Copilot, familiarize themselves with its applications, and engage with the ethical and data protection issues it raises. Through practical application within the project, they are empowered to effectively use Copilot in various professional contexts, optimize processes, and develop innovative solutions for complex problems. The critical examination of the potential and limitations of this technology also promotes a deep understanding of the responsibility that comes with the use of AI.

Course Outcomes

On successful completion, students will be able to

- understand the basic functions and applications of Microsoft Copilot, including in the fields of text generation and data analysis.
- recognize the possibilities for automating work processes using Copilot and its contribution to efficiency improvement.
- understand interdisciplinary collaboration with Copilot.
- identify and evaluate potential application areas of Copilot in a professional context.
- understand and discuss ethical and data protection aspects of using Copilot.
- develop a critical reflection on the advantages and disadvantages of using Copilot.

Contents

- In this course, students engage deeply with Microsoft Copilot by exploring its applications in practical, real-world scenarios. Through independent experimentation, they learn how Copilot can contribute to the automation of routine tasks, generate complex texts, and perform extensive data analyses. As part of the course, students are encouraged to design their own projects where they use Copilot to solve specific challenges. Emphasis is also placed on the consideration of ethical principles and data protection regulations. By participating in the offered exchange opportunities, students can further develop their critical awareness of the social impacts of AI usage. This course lays the foundation

for a thorough understanding of the possibilities and limitations of AI-powered work processes and prepares students to responsibly handle the challenges of the digitalized work environment.

Literature
Compulsory Reading
Further Reading ▪ Khan, A. (2024). Introducing Microsoft Copilot for managers: Enhance your team's productivity and creativity with generative AI-powered assistant. Apress. ▪ Microsoft. (2024). Explore how to use Microsoft 365 Copilot. ▪ Microsoft. (2024). Official Microsoft 365 Copilot for Service documentation. ▪ Narayanaswamy, A. (2024). Microsoft Copilot for Windows 11: Understanding the AI-powered features in Windows 11. Apress. ▪ Stratton, J. (2024). Copilot for Microsoft 365: Harness the power of generative AI in the Microsoft apps you use every day. Apress.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods

Tutorial Support
☑ Course Feed
☑ Intensive Live Sessions/Learning Sprint
☑ Recorded Live Sessions

Exam Preparation
☑ Guideline

Studium Generale V und VI

Modulcode: DLBSGFUS

Modultyp	Zugangsvoraussetzungen	Niveau	CP	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)

N.N. (Studium Generale V) / N.N. (Studium Generale VI)

Kurse im Modul

- Studium Generale V (DLBSG05)
- Studium Generale VI (DLBSG06)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Studium Generale V • Studienformat "Duales myStudium": Siehe gewählter Kurs • Studienformat "Fernstudium": Siehe gewählter Kurs Studium Generale VI • Studienformat "Duales myStudium": Siehe gewählter Kurs • Studienformat "Fernstudium": Siehe gewählter Kurs

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Studium Generale V

Als Kurs für das „Studium Generale“ sind prinzipiell alle IU-Bachelorkurse wählbar, sodass inhaltlich aus der gesamten Breite des IU Fernstudiums gewählt werden kann.

Studium Generale VI

Als Kurs für das „Studium Generale“ sind prinzipiell alle IU-Bachelorkurse wählbar, sodass inhaltlich aus der gesamten Breite des IU Fernstudiums gewählt werden kann.

Qualifikationsziele des Moduls

Studium Generale V

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 VI

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	**Bezüge zu anderen Studiengängen der Hochschule**
Ist ein eigenständiges Angebot mit möglichen Bezügen zu verschiedenen Pflicht- und Wahlpflichtmodulen	Alle Bachelor-Programme des IU Fernstudiums

Studium Generale V

Kurscode: DLBSG05

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

Beschreibung des Kurses

Im Rahmen des Kurses „Studium Generale V“ vertiefen die Studierenden ihr Wissen in einem selbstgewählten Themenfeld durch das Absolvieren eines IU-Kurses außerhalb ihres geltenden Curriculums. Sie haben dadurch die Möglichkeit, ihr Wissen innerhalb ihres Fachgebietes weiter zu vertiefen und/oder über den Tellerrand 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 und die Arbeitswelt 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 V“ 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.

Literatur

Pflichtliteratur

Weiterführende Literatur

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studium Generale VI

Kurscode: DLBSG06

Niveau	Kurs- und Prüfungssprache	SWS	CP	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, ihr Wissen innerhalb ihres Fachgebietes weiter zu vertiefen und/oder über den Tellerrand 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 und die Arbeitswelt 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 VI“ 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.

Literatur

Pflichtliteratur

Weiterführende Literatur

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Siehe gewählter Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Siehe gewählter Kurs

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	0 h	0 h	0 h	0 h

Lehrmethoden
Siehe Kursbeschreibung des gewählten Kurses

Bachelorarbeit

Modulcode: BBAK

Modultyp	Zugangsvoraussetzungen	Niveau	CP	Zeitaufwand Studierende
s. Curriculum	gemäß Studien- und Prüfungsordnung	BA	10	300 h

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

Modulverantwortliche(r)

Prof. Dr. Cornelia Schlick (Bachelorarbeit) / Prof. Dr. Christian Müller-Kett (Kolloquium)

Kurse im Modul

- Bachelorarbeit (BBAK01)
- Kolloquium (BBAK02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Bachelorarbeit • Studienformat "Duales myStudium": Schriftliche Ausarbeitung: Bachelorarbeit • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Bachelorarbeit • Studienformat "myStudium": Schriftliche Ausarbeitung: Bachelorarbeit • Studienformat "Duales Studium": Bachelorarbeit • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Bachelorarbeit Kolloquium • Studienformat "myStudium": Kolloquium • Studienformat "Duales Studium": Kolloquium • Studienformat "Duales 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	**Bezüge zu anderen Studiengängen der Hochschule**
Alle Module	Alle Bachelor-Programme im Fernstudium

Bachelorarbeit

Kurscode: BBAK01

Niveau	Kurs- und Prüfungssprache	SWS	CP	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 Bedürfnissen 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 ▪ Hemmer, M. C., & Fröhlich, T. (2023). The Art of Thesis Writing. ▪ 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 Literaturauswahl

Studienformat Duales myStudium

Studienform	**Kursart**
Duales myStudium	Thesis-Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Bachelorarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
270 h	0 h	0 h	0 h	0 h	270 h

Lehrmethoden
Selbstständige Projektbearbeitung unter akademischer Anleitung.

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Bachelorarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
270 h	0 h	0 h	0 h	0 h	270 h

Lehrmethoden
Selbstständige Projektbearbeitung unter akademischer Anleitung.

Studienformat myStudium

Studienform	Kursart
myStudium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Bachelorarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
270 h	0 h	0 h	0 h	0 h	270 h

Lehrmethoden
Selbstständige Projektbearbeitung unter akademischer Anleitung.

Studienformat Duales Studium

Studienform	**Kursart**
Duales Studium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Bachelorarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium/ synchrone virtuelle Lehre**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
270 h	0 h	0 h	0 h	0 h	270 h

Lehrmethoden
Selbstständige Projektbearbeitung unter akademischer Anleitung.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Bachelorarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
270 h	0 h	0 h	0 h	0 h	270 h

Lehrmethoden
Selbstständige Projektbearbeitung unter akademischer Anleitung.

Kolloquium

Kurscode: BBAK02

Niveau	Kurs- und Prüfungssprache	SWS	CP	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

- Hemmer, M. C., & Fröhlich, T. (2023). The Art of Thesis Writing.
- Renz, K.-C. (2016): Das 1 x 1 der Präsentation. Für Schule, Studium und Beruf. 2. Auflage, Springer Gabler, Wiesbaden.

Studienformat myStudium

Studienform	Kursart
myStudium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Kolloquium

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
30 h	0 h	0 h	0 h	0 h	30 h

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung

Studienformat Duales Studium

Studienform	**Kursart**
Duales Studium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Kolloquium

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium/ synchrone virtuelle Lehre**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
30 h	0 h	0 h	0 h	0 h	30 h

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung.

Studienformat Duales myStudium

Studienform	Kursart
Duales myStudium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Kolloquium

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
0 h	0 h	30 h	0 h	0 h	30 h

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Kolloquium

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
30 h	0 h	0 h	0 h	0 h	30 h

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Abschlussarbeit

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**Online Tests:** Nein
Prüfungsleistung	Kolloquium

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium/ Tutorielle Betreuung**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
30 h	0 h	0 h	0 h	0 h	30 h

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung