

MODULHANDBUCH

Master of Science

Master Cyber Security (FS-MACSD-120)

120 CP

Fernstudium

Stand: 23.April 2024

Klassifizierung: Konsekutiv

Inhaltsverzeichnis

1. Semester

Modul DLMIGCR-01: IT-Governance, -Compliance und -Recht

Modulbeschreibung	8
Kurs DLMIGCR01-01: IT-Governance, -Compliance und -Recht	10

Modul DLMDWWM: Weiterführende Mathematik

Modulbeschreibung	13
Kurs DLMDWWM01: Weiterführende Mathematik	15

Modul DLMCSITSDS: IT-Sicherheit und Datenschutz

Modulbeschreibung	18
Kurs DLMCSITSDS01: IT-Sicherheit und Datenschutz	20

Modul DLMMET-02: Forschungsmethodik

Modulbeschreibung	24
Kurs MMET01-02: Forschungsmethodik	26

Modul DLMCSSAITS_D: Seminar: Fortgeschrittene IT-Sicherheit

Modulbeschreibung	31
Kurs DLMCSEAITSC01_D: Seminar: Fortgeschrittene IT-Sicherheit	33

Modul DLMCSC_D: Kryptologie

Modulbeschreibung	36
Kurs DLMCSEAITSC02_D: Kryptologie	38

2. Semester

Modul DLMCSECRAM_D: Cyber Risk Assessment und Management

Modulbeschreibung	43
Kurs DLMCSECRAM01_D: Cyber Risk Assessment und Management	45

Modul DLMIMITSS: IT-Systeme: Software

Modulbeschreibung	48
Kurs DLMIMITSS01: IT-Systeme: Software	50

Modul DLMIMITSH: IT-Systeme: Hardware

Modulbeschreibung	54
Kurs DLMIMITSH01: IT-Systeme: Hardware	56

Modul DLMCSECSNF_D: Cybersysteme und Netzwerkforensik

Modulbeschreibung	60
Kurs DLMCSECSNF01_D: Cybersysteme und Netzwerkforensik	62

Modul DLMCSEESN1_D: Netzwerksicherheit

Modulbeschreibung	65
Kurs DLMCSEESN01_D: Netzwerksicherheit	67

Modul DLMCSETCSITS_D: Theoretische Informatik für IT-Sicherheit

Modulbeschreibung	71
Kurs DLMCSETCSITS01_D: Theoretische Informatik für IT-Sicherheit	73

3. Semester**Modul DLMIMSSF: Seminar: Standards und Frameworks**

Modulbeschreibung	78
Kurs DLMIMSSF01: Seminar: Standards und Frameworks	80

Modul DLMCSEPCCS_D: Projekt: Aktuelle Herausforderungen der Cyber-Sicherheit

Modulbeschreibung	83
Kurs DLMCSEPCCS01_D: Projekt: Aktuelle Herausforderungen der Cyber-Sicherheit	85

Modul DLMIMWCK: Computerkriminalität

Modulbeschreibung	88
Kurs DLMIMWCK01: Angriffsszenarien und Vorfalreaktion	90
Kurs DLMIMWCK02: Projekt: Cyber-Forensik	94

Modul DLMCSEBCQC: Blockchain and Quantum Computing

Modulbeschreibung	97
Kurs DLMCSEBCQC01: Blockchain	99
Kurs DLMCSEBCQC02: Quantum Computing	103

Modul DLMCSEEDSO_D: Sichere Software-Entwicklung

Modulbeschreibung	107
Kurs DLMCSEEDSO01_D: Sichere Software-Entwicklung	109
Kurs DLMCSEEDSO02_D: Projekt: Sichere Software-Implementierung	112

Modul DLMCSDWTO_D: Transformation von Organisationen

Modulbeschreibung	114
Kurs DLMWPWOAE01: Instrumente der Organisationsanalyse	117
Kurs MWIT02: Management von IT-Services und IT-Architekturen	121

Modul DLMCSEETLS_D: IT-Recht in der IT-Sicherheit

Modulbeschreibung	125
-------------------------	-----

Kurs DLMIMWITR01: Nationales und internationales IT-Recht	128
Kurs DLMCSEEITLS01_D: Seminar: Rechtliche Rahmenbedingungen der IT-Sicherheit	132

Modul DLMCSEEAST_E: Audit- and Security Testing

Modulbeschreibung	135
Kurs DLMCSEEAST01_E: Attack Models and Auditing	137
Kurs DLMCSEEAST02_E: Seminar: IT Security Tests	140

Modul DLMDWWBA: Business Analyst

Modulbeschreibung	143
Kurs DLMIWBI01: Business Intelligence I	145
Kurs DLMDWWBA01: Projekt: Business Intelligence	148

Modul DLMCSEECLS_E: Continuous and Lifecycle Security

Modulbeschreibung	151
Kurs DLMCSEECLS01_E: Cyber Resilience	153
Kurs DLMCSEECLS02_E: Seminar: Applying Threat Intelligence	157

Modul DLMCSEEDSBDT_D: Data Science und Big Data Technologien

Modulbeschreibung	159
Kurs DLMDWDS01: Data Science	161
Kurs DLMDWBDT01: Big-Data-Technologien	164

Modul DLMDWWATIOT: Automatisierungstechnik und Internet of Things

Modulbeschreibung	167
Kurs DLMDWAUTT01: Automatisierungstechnik	170
Kurs DLMDWWIOT01: Internet of Things	174

Modul DLMIMWKI_D: Künstliche Intelligenz

Modulbeschreibung	177
Kurs DLMAIAI01_D: Künstliche Intelligenz	180
Kurs DLMAISAI01_D: Seminar: Künstliche Intelligenz und Gesellschaft	183

Modul DLMEAIMAIP: AI and Mastering AI Prompting

Modulbeschreibung	186
Kurs DLMAIAI01: Artificial Intelligence	188
Kurs DLMPAIECPT01: Project: AI Excellence with Creative Prompting Techniques	192

4. Semester

Modul MMTH: Masterarbeit

Modulbeschreibung	196
Kurs MMTH01: Masterarbeit	198

Kurs MMTH02: Kolloquium 201

1. Semester

IT-Governance, -Compliance und -Recht

Modulcode: DLMIGCR-01

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

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

Modulverantwortliche(r)

Carsten Pauck (IT-Governance, -Compliance und -Recht)

Kurse im Modul

- IT-Governance, -Compliance und -Recht (DLMIGCR01-01)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur, 90 Minuten

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- IT-Governance: Motivation und Herausforderungen
- COBIT-Framework
- IT-Compliance
- IT-Grundschutz nach BSI
- IT-Recht

Qualifikationsziele des Moduls**IT-Governance, -Compliance und -Recht**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Begriffe IT-Governance und IT-Compliance zu erläutern.
- typische Prozesse und Aktivitäten aus dem Bereich IT-Governance und IT-Compliance zu kategorisieren.
- einen Überblick über das Framework COBIT und seine Elemente zu geben.
- einen Überblick über den IT-Grundschutz zu geben und dessen Aufbau zu erklären.
- wichtige Gesetze und Vorschriften aus dem Bereich IT-Recht wiederzugeben und deren Anwendungsgebiete zu erläutern.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik

IT-Governance, -Compliance und -Recht

Kurscode: DLMIGCR01-01

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

Beschreibung des Kurses

In diesem Kurs lernen die Studierenden Begriffe und Frameworks rund um die Themen IT-Governance und IT-Compliance kennen. Nach einer kurzen Einführung und einem Überblick über die verschiedenen Aspekte von IT-Governance und IT-Compliance werden mit COBIT und dem IT-Grundschutz zwei Rahmenwerke vorgestellt, die in der industriellen Praxis zum Einsatz kommen. Darüber hinaus werden in diesem Kurs wichtige rechtliche Rahmenbedingungen und Normen rund um das Thema IT-Recht vorgestellt und diskutiert.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Begriffe IT-Governance und IT-Compliance zu erläutern.
- typische Prozesse und Aktivitäten aus dem Bereich IT-Governance und IT-Compliance zu kategorisieren.
- einen Überblick über das Framework COBIT und seine Elemente zu geben.
- einen Überblick über den IT-Grundschutz zu geben und dessen Aufbau zu erklären.
- wichtige Gesetze und Vorschriften aus dem Bereich IT-Recht wiederzugeben und deren Anwendungsgebiete zu erläutern.

Kursinhalt

1. IT-Governance: Motivation und Herausforderungen
 - 1.1 Begriff: Governance und IT-Governance
 - 1.2 Rahmenbedingungen für IT-Governance
 - 1.3 Typische IT-Governance-Frameworks
2. COBIT-Framework
 - 2.1 Überblick über die Elemente von COBIT
 - 2.2 Die Zielkaskade von COBIT
 - 2.3 Governance- und Management-Ziele (Governance and Management Objectives)
 - 2.4 Einsatz von COBIT
3. IT-Compliance
 - 3.1 IT-Compliance und IT-Governance

- 3.2 Beispiele für nationale und internationale Richtlinien
- 3.3 Typische Maßnahmen
- 4. IT-Grundschutz nach BSI
 - 4.1 Überblick und Aufbau
 - 4.2 Die Vorgehensweise zum IT-Grundschutz
 - 4.3 Nutzungsbeispiel des IT-Grundschutzes
- 5. IT-Recht
 - 5.1 Überblick über relevante Gesetze
 - 5.2 Schutz des geistigen Eigentums
 - 5.3 IT-Verträge
 - 5.4 Datenschutz

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bundesamt für Sicherheit in der Informationstechnik (2018): IT-Grundschutz-Kompendium. (URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html [letzter Zugriff: 26.04.2018]).
- Falk, M. (2012): IT-Compliance in der Corporate Governance. Anforderungen und Umsetzung. Springer Gabler, Wiesbaden.
- Gaulke, M. (2014): Praxiswissen COBIT. Grundlagen und praktische Anwendung in der Unternehmens-IT. 2. Auflage, dpunkt.verlag, Heidelberg.
- Grünendahl, R. T./Steinbacher, A. F./Will, P. (2012): Das IT-Gesetz. Compliance in der IT-Sicherheit. Leitfaden für ein Regelwerk zur IT-Sicherheit im Unternehmen. 2. Auflage, Springer Vieweg, Wiesbaden.
- Harmer, G. (2014): Governance of Enterprise IT based on COBIT 5. A Management Guide. itgp, Ely (UK).
- ISACA (Hrsg.) (2012): COBIT 5. A Business Framework for the Governance and Management of Enterprise IT. Isaca, Berlin.
- ISACA (2018): COBIT® 2019 Framework: Introduction & Methodology. Isaca, Schaumburg IL.
- Johannsen, W./Goeken, M. (2010): Referenzmodelle für IT-Governance. Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co. 2. Auflage, dpunkt.verlag, Heidelberg.
- Nitsch, K. W. (2014): IT-Recht. 4. Auflage, EHV Academicpress, Bremen.
- Weill, P./Ross, J. W. (2004): IT Governance. How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business Review Press, Watertown (MA).

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Musterklausur <input checked="" type="checkbox"/> Online Tests

Weiterführende Mathematik

Modulcode: DLMDWWM

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

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

Modulverantwortliche(r)

Prof. Dr. Robert Graf (Weiterführende Mathematik)

Kurse im Modul

- Weiterführende Mathematik (DLMDWWM01)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur, 90 Minuten

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Kalkül
- Integrale Transformationen
- Vektoralgebra
- Vektorrechnung
- Matrizen und Vektorräume
- Informationstheorie

Qualifikationsziele des Moduls**Weiterführende Mathematik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sich an die Grundregeln der Differenzierung und Integration zu erinnern.
- Integrations- und Differenzierungstechniken auf Vektoren und Vektorfelder anzuwenden.
- Matrixgleichungen zu analysieren.
- die Verallgemeinerung von Vektoren zu Tensoren zu verstehen.
- verschiedene Metriken aus informationstheoretischer Sicht zu bewerten.

Bezüge zu anderen Modulen im Studiengang

Ist Grundlage für weitere Module im Bereich Methoden

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich Wirtschaft & Management

Weiterführende Mathematik

Kurscode: DLMDWWM01

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

Beschreibung des Kurses

Moderne Techniken zur Datenanalyse und zur Ableitung von Vorhersagen für zukünftige Ereignisse sind tief in mathematischen Techniken verwurzelt. Der Kurs bildet eine solide Grundlage, um die Konzepte hinter fortschrittlichen Algorithmen zur Verarbeitung, Analyse und Vorhersage von Daten und Beobachtungen zu verstehen und ermöglicht es den Studierenden, zukünftige Forschungsarbeiten, insbesondere in den Bereichen der datenintensiven Wissenschaften, zu verfolgen. Der Kurs behandelt Differenzierung und Integration und diskutiert dann partielle Differenzierung, Differenzierung, Vektoralgebra und Vektorrechnung. Matrixberechnung und Vektorräume sind die Grundlage für viele moderne Datenverarbeitungsalgorithmen und werden ausführlich diskutiert. Es werden Berechnungen auf Basis von Tensoren vorgestellt. Gängige Metriken werden aus informativer, theoretischer Sicht diskutiert.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sich an die Grundregeln der Differenzierung und Integration zu erinnern.
- Integrations- und Differenzierungstechniken auf Vektoren und Vektorfelder anzuwenden.
- Matrixgleichungen zu analysieren.
- die Verallgemeinerung von Vektoren zu Tensoren zu verstehen.
- verschiedene Metriken aus informationstheoretischer Sicht zu bewerten.

Kursinhalt

1. Kalkül
 - 1.1 Differenzierung & Integration
 - 1.2 Teilweise Differenzierung & Integration
 - 1.3 Vektoranalyse
 - 1.4 Variationsrechnung
2. Integrale Transformationen
 - 2.1 Faltung
 - 2.2 Fourier-Transformation
3. Vektor-Algebra
 - 3.1 Skalare und Vektoren

- 3.2 Addition, Subtraktion von Vektoren
- 3.3 Multiplikation von Vektoren, Vektorprodukt, Skalarprodukt
- 4. Vektorrechnung
 - 4.1 Integration von Vektoren
 - 4.2 Differenzierung von Vektoren
 - 4.3 Skalare und Vektorfelder
 - 4.4 Vektor-Operatoren
- 5. Matrizen und Vektorräume
 - 5.1 Grundlegende Matrix Algebra
 - 5.2 Determinante, Spuren, Transponierte, Komplexe und Hermitianische Konjugate
 - 5.3 Eigenvektoren und Eigenwerte
 - 5.4 Diagonalisierung
 - 5.5 Tensoren
- 6. Informationstheorie
 - 6.1 MSE
 - 6.2 Gini-Index
 - 6.3 Entropie, Shannon-Entropie, Kulback Leibler Distanz
 - 6.4 Kreuzentropie

Literatur

Pflichtliteratur

Weiterführende Literatur

- Haubold, H. J., & Mathai, A. M. (2017). Linear Algebra. A Course for Physicists and Engineers. De Gruyter.
- Hoever, G. V. (2020): Höhere Mathematik kompakt mit Erklärvideos und interaktiven Visualisierungen. Springer, Berlin/Heidelberg.
- Riley, K. F./Hobson, M. P./Bence, S. J. (2006): Mathematical methods for physics and engineering. 3. Auflage, University Press, Cambridge.
- Weißgerber, W. (2023): Mathematik zu Elektrotechnik für Ingenieure. Lehr- und Arbeitsbuch für das Grundstudium. Springer Vieweg, Wiesbaden.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

IT-Sicherheit und Datenschutz

Modulcode: DLMCSITSDS

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

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

Modulverantwortliche(r)

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

Kurse im Modul

- IT-Sicherheit und Datenschutz (DLMCSITSDS01)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Fachpräsentation

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Datenschutz und Privatsphäre
- Bausteine der IT-Sicherheit
- IT-Sicherheitsmanagement
- Kryptographiekonzepte
- Kryptographie-Anwendungen

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

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Kernkonzepte von IT-Sicherheit, Datenschutz und Kryptographie einschließlich ihrer Unterschiede und Beziehungen zu erklären.
- die Ansätze zum Datenschutz in verschiedenen Rechtsordnungen zu vergleichen.
- Datenschutzkonzepte auf die Datenwissenschaft und andere Anwendungsszenarien anzuwenden.
- eine Analyse von Anwendungsszenarien durchzuführen, um die geeigneten Maßnahmen für das IT-Sicherheitsmanagement zu identifizieren, die umgesetzt werden sollten.
- Anwendungsszenarien zu untersuchen, um die geeigneten kryptografischen Konzepte zu identifizieren.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik

IT-Sicherheit und Datenschutz

Kurscode: DLMCSITSDS01

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

Beschreibung des Kurses

Mit der zunehmenden Digitalisierung und Vernetzung von IT-Systemen ist der Bedarf gestiegen, Systeme und die von diesen Systemen verarbeiteten Daten zu schützen. Ziel dieses Moduls ist es, ein Verständnis für die erforderlichen Sicherheitsmaßnahmen, die IT-Sicherheit einschließlich Kryptographie und den Datenschutz zu vermitteln. Während der Bedarf an IT-Sicherheit weltweit ähnlich ist, haben verschiedene Kulturen unterschiedliche Erwartungen an Datenschutz und Privatsphäre. Dennoch werden personenbezogene Daten oft außerhalb des Landes verarbeitet, in dem die betroffenen Personen leben. Daher müssen die kulturellen Aspekte des Datenschutzes bei der Verarbeitung der Daten berücksichtigt werden. Dieser Kurs gibt einen Überblick über die wichtigsten IT-Sicherheitsmaßnahmen in verschiedenen Anwendungsszenarien sowie deren Integration in ein Informationssicherheitsmanagementsystem mit besonderem Fokus auf die relevante Normenfamilie ISO/IEC 270xx. Die Kryptographie stellt ein wichtiges Werkzeug für die IT-Sicherheit dar und wird in vielen verschiedenen Anwendungsszenarien wie sicheren Internetprotokollen und Block Chain eingesetzt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Kernkonzepte von IT-Sicherheit, Datenschutz und Kryptographie einschließlich ihrer Unterschiede und Beziehungen zu erklären.
- die Ansätze zum Datenschutz in verschiedenen Rechtsordnungen zu vergleichen.
- Datenschutzkonzepte auf die Datenwissenschaft und andere Anwendungsszenarien anzuwenden.
- eine Analyse von Anwendungsszenarien durchzuführen, um die geeigneten Maßnahmen für das IT-Sicherheitsmanagement zu identifizieren, die umgesetzt werden sollten.
- Anwendungsszenarien zu untersuchen, um die geeigneten kryptografischen Konzepte zu identifizieren.

Kursinhalt

1. Grundlagen von Datenschutz und IT-Sicherheit
 - 1.1 Terminologie und Risikomanagement
 - 1.2 Kernkonzepte der IT-Sicherheit
 - 1.3 Kernkonzepte von Datenschutz und Privatsphäre
 - 1.4 Kernkonzepte der Kryptografie

- 1.5 Rechtliche Aspekte
2. Datenschutz
 - 2.1 Grundbegriffe des Datenschutzes (ISO/IEC 29100, Privacy by Design)
 - 2.2 Datenschutz in Europa: die DSGVO
 - 2.3 Datenschutz in den USA
 - 2.4 Datenschutz in Asien
3. Anwendung des Datenschutzes
 - 3.1 Anonymität und Pseudonyme
 - 3.2 Datenschutz in der Datenwissenschaft und Big Data
 - 3.3 Benutzer-Tracking im Online-Marketing
 - 3.4 Cloud Computing
4. Bestandteile der IT-Sicherheit
 - 4.1 Authentifizierung, Zugriffsverwaltung und -kontrolle
 - 4.2 Endgerätesicherheit
 - 4.3 IT-Sicherheit in Netzwerken
 - 4.4 Entwicklung sicherer IT-Systeme
5. IT-Sicherheitsmanagement
 - 5.1 Sicherheitsrichtlinien
 - 5.2 Sicherheits- und Risikoanalyse
 - 5.3 Die ISO 27000-Reihe
 - 5.4 IT-Sicherheit und IT-Governance
 - 5.5 Beispiel: IT-Sicherheit für Kreditkarten (PCI DSS)
6. Kryptografie
 - 6.1 Grundbegriffe der Kryptografie
 - 6.2 Symmetrische Kryptografie
 - 6.3 Asymmetrische Kryptografie
 - 6.4 Kryptografie mit elliptischer Kurve
 - 6.5 Hash-Funktionen
 - 6.6 Sicherer Datenaustausch
7. Kryptografische Anwendung
 - 7.1 Digitale Signaturen
 - 7.2 Sichere Internet-Protokolle
 - 7.3 Blockchain

7.4 Elektronisches Geld

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

- Bowman, C. et al. (2015): The architecture of privacy. On engineering technologies that can deliver trustworthy safeguards. O'Reilly, Sebastopol, CA.
- Hintzbergen, J. et al. (2015): Foundations of information security (3rd ed.). Van Haren Publishing, Zaltbommel.
- ISO/IEC 29100 (2011): Information technology — Security techniques — Privacy framework. ISO. (URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip [Retrieved: 11.3.2020]).
- Paar, C./Pelzl, J. (2011). Understanding cryptography: A textbook for students and practitioners. Springer, Heidelberg.
- The Open Web Application Security Project (OWASP) (2005): A guide to building secure web applications and web services. OWASP. (URL: <https://www.um.es/atika/documentos/OWASPGuide2.0.1.pdf> [Retrieved: 11.3.2020]).

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	Online Tests: Ja
Prüfungsleistung	Fachpräsentation

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Online Tests <input checked="" type="checkbox"/> Prüfungsleitfaden

Forschungsmethodik

Modulcode: DLMMET-02

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

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

Modulverantwortliche(r)

Prof. Dr. Julia Pitters (Forschungsmethodik)

Kurse im Modul

- Forschungsmethodik (MMET01-02)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Schriftliche Ausarbeitung: Hausarbeit

Studienformat: Kombistudium
Schriftliche Ausarbeitung: Hausarbeit

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Einführung in Wissenschaftstheorien
- Voraussetzungen für quantitatives Messen und Testen
- Grundlagen der qualitativen Forschung

Qualifikationsziele des Moduls

Forschungsmethodik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- zwischen qualitativer und quantitativer Forschung zu differenzieren.
- die methodologischen Voraussetzungen zu bestimmen, die bei der quantitativen Messung und Testung spezifischer Konstrukte gegeben sein müssen.
- die jeweiligen quantitativen Skalen und Indikatoren zielgerichtet in eigener Forschung einzusetzen.
- verschiedene qualitative Erhebungs- und Auswertungsverfahren voneinander zu unterscheiden und in eigener Forschung anzuwenden.
- spezielle Probleme bei der Durchführung von Forschungsstudien zu analysieren und Lösungsvorschläge zu erarbeiten.
- die Qualität von Forschungsvorhaben hinsichtlich quantitativer und qualitativer Gütekriterien bewerten zu können.
- Konzeptionen der Forschung im Hinblick auf Forschungsphilosophie, Forschungsfrage, Forschungsansatz, Darstellung und ethischen Aspekten zu bewerten.

Bezüge zu anderen Modulen im Studiengang

Ist Grundlage für alle weiteren Module im Bereich Methoden

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich Wirtschaft & Management

Forschungsmethodik

Kurscode: MMET01-02

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

Beschreibung des Kurses

Auf Basis eines wissenschaftstheoretischen Hintergrunds erlernen die Studierenden zunächst sowohl die Terminologie als auch die forschungstheoretischen Paradigmen kennen. Anschließend geht es um die Differenzierung von klassischen quantitativen versus qualitativen Forschungsmethoden mit ihren jeweiligen Vor- und Nachteilen sowie um die Betrachtung der Gütekriterien. Auf den Annahmen der klassischen sowie der probabilistischen Testtheorie beruhend, werden die Voraussetzungen für die Konstruktion einer quantitativen Studie besprochen, die wichtigsten Forschungsmethoden vorgestellt und die einzelnen Schritte eines Forschungsprojekts nachvollzogen. Des Weiteren erfolgt die Befassung mit den relevantesten qualitativen Forschungs- und Auswertungsmethoden. Den Abschluss bildet eine kritische Auseinandersetzung hinsichtlich ethischer und datenschutzrechtlicher Aspekte empirischer (digitaler) Forschung.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- zwischen qualitativer und quantitativer Forschung zu differenzieren.
- die methodologischen Voraussetzungen zu bestimmen, die bei der quantitativen Messung und Testung spezifischer Konstrukte gegeben sein müssen.
- die jeweiligen quantitativen Skalen und Indikatoren zielgerichtet in eigener Forschung einzusetzen.
- verschiedene qualitative Erhebungs- und Auswertungsverfahren voneinander zu unterscheiden und in eigener Forschung anzuwenden.
- spezielle Probleme bei der Durchführung von Forschungsstudien zu analysieren und Lösungsvorschläge zu erarbeiten.
- die Qualität von Forschungsvorhaben hinsichtlich quantitativer und qualitativer Gütekriterien bewerten zu können.
- Konzeptionen der Forschung im Hinblick auf Forschungsphilosophie, Forschungsfrage, Forschungsansatz, Darstellung und ethischen Aspekten zu bewerten.

Kursinhalt

1. Wissenschaftliche Grundlagen
 - 1.1 Grundlegende Vorstellungen in der Wissenschaft
 - 1.2 Erklärungsansätze in der Wissenschaft
 - 1.3 Perspektiven in der Wissenschaft

2. Forschungsrichtungen und Gütekriterien
 - 2.1 Quantitative versus qualitative Forschung
 - 2.2 Gütekriterien in der quantitativen und qualitativen Forschung
3. Test- und Fragebogenkonstruktion
 - 3.1 Skalenniveaus und die Unterscheidung manifester und latenter Merkmale
 - 3.2 Klassische Testtheorie
 - 3.3 Probabilistische Testtheorie
 - 3.4 Grundlegende Konzepte der Itembildung
 - 3.5 Skalierungsverfahren und Indexbildung
4. Quantitatives Forschungsdesign
 - 4.1 Die Befragung
 - 4.2 Das Experiment
 - 4.3 Die Beobachtung
5. Qualitatives Forschungsdesign
 - 5.1 Das Interview
 - 5.2 Die Fokusgruppe
 - 5.3 Grounded Theory
6. Umsetzung, Darstellung und Reflexion
 - 6.1 Forschungsplan/Exposé
 - 6.2 Dokumentation des Forschungsprozesses
 - 6.3 Darstellung von Forschungsergebnissen
 - 6.4 Interpretation von Forschungsergebnissen
 - 6.5 Ethische Aspekte, digitale Entwicklungen und Datenschutz

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

- Bortz, J./Döring, N. (2006). Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler. 4. Auflage, Springer, Heidelberg.
- Diekmann, A. (2007). Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen. 4. Auflage, Rowohlt, Reinbek.
- Kromrey, H. (2009). Empirische Sozialforschung. 12. Auflage, UTB, Stuttgart.
- Lamnek, S. (2010). Qualitative Sozialforschung. 5. Auflage, Beltz, Weinheim.
- Mayring, P. (2002). Einführung in die Qualitative Sozialforschung. 5. Auflage, Beltz, Weinheim.
- Mayring, P. (2010). Qualitative Inhaltsanalyse. Grundlagen und Techniken. 11. Auflage, Beltz, Weinheim.
- Schnell, R./Hill, P. B./Esser, E. (2008). Methoden der empirischen Sozialforschung. 8. Auflage, Oldenbourg, München.
- Sedlmeier, P./Renkewitz, F. (2007). Forschungsmethoden und Statistik in der Psychologie. Pearson Studium, München.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Repetitorium <input checked="" type="checkbox"/> Online Tests <input checked="" type="checkbox"/> Prüfungsleitfaden

Studienformat Kombistudium

Studienform Kombistudium	Kursart Theoriekurs
------------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Repetitorium <input checked="" type="checkbox"/> Online Tests <input checked="" type="checkbox"/> Prüfungsleitfaden

Seminar: Fortgeschrittene IT-Sicherheit

Modulcode: DLMCSAITS_D

Modultyp s. Curriculum	Zugangsvoraussetzungen DLMCSITSDP01 oder DLMCSITSDS01	Niveau MA	CP 5	Zeitaufwand Studierende 150 h
----------------------------------	--	---------------------	----------------	---

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

Modulverantwortliche(r)

Petra Beenken (Seminar: Fortgeschrittene IT-Sicherheit)

Kurse im Modul

- Seminar: Fortgeschrittene IT-Sicherheit (DLMCSAITS_D)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Schriftliche Ausarbeitung: Seminararbeit

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

In diesem Kurs beschäftigen sich die Studierenden mit verschiedenen fortgeschrittenen Themen der Cyber Security einschließlich der verwandten Themen Datensicherheit und Kryptologie und diskutieren diese im Detail.

Qualifikationsziele des Moduls**Seminar: Fortgeschrittene IT-Sicherheit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einen Aspekt der Cyber Security im Detail zu analysieren und zu beschreiben.
- ausgewählte Themen der Cyber Security selbstständig zu analysieren und mit bekannten Konzepten zu verknüpfen sowie kritisch zu hinterfragen und zu diskutieren.
- theoretisch erworbenes Wissen auf einen spezifischen Kontext zu übertragen.
- eine wissenschaftliche Arbeit über ein relevantes ausgewähltes Thema zu schreiben und zu bearbeiten.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik

Seminar: Fortgeschrittene IT-Sicherheit

Kurscode: DLMCSEAITSC01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
MA	Deutsch		5	DLMCSITSDP01 oder DLMCSITSDS01

Beschreibung des Kurses

Dieser Kurs behandelt fortgeschrittene Themen der Cyber Security. Mit dem Wachstum des Internets und der Digitalisierung ist Cyber Security ein immer wichtigeres Thema geworden und muss bei der Entwicklung und Einrichtung von Software und IT-Systemen berücksichtigt werden. Typische Themen, die behandelt werden können, sind die Analyse ausgewählter Aspekte von Informationssicherheits-Managementsystemen nach der ISO 27000er-Reihe, der Nutzen von Cyber Security zur Unterstützung des Datenschutzes sowie die detaillierte Analyse und Beschreibung bestimmter Algorithmen oder Kryptosysteme.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einen Aspekt der Cyber Security im Detail zu analysieren und zu beschreiben.
- ausgewählte Themen der Cyber Security selbstständig zu analysieren und mit bekannten Konzepten zu verknüpfen sowie kritisch zu hinterfragen und zu diskutieren.
- theoretisch erworbenes Wissen auf einen spezifischen Kontext zu übertragen.
- eine wissenschaftliche Arbeit über ein relevantes ausgewähltes Thema zu schreiben und zu bearbeiten.

Kursinhalt

- In diesem Kurs beschäftigen sich die Studierenden mit verschiedenen fortgeschrittenen Themen der Cyber Security einschließlich der verwandten Themen Datensicherheit und Kryptologie und diskutieren diese im Detail. Jeder Teilnehmer muss eine Seminararbeit zu einem ausgewählten Thema schreiben.

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

- Bowman, C. et al. (2015): The architecture of privacy. On engineering technologies that can deliver trustworthy safeguards. O'Reilly, Sebastopol, CA.
- Hintzbergen, J. et al. (2015): Foundations of information security. 3rd Edition, Van Haren Publishing, Zaltbommel.
- ISO/IEC 29100. (2011): Information technology – Security techniques – Privacy framework. ISO. (URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip [Retrieved: 11.03.2021]).
- Paar, C./Pelzl, J. (2011): Understanding cryptography. A textbook for students and practitioners. Springer, Heidelberg.
- Schmeh, K. (2016): Kryptografie. Verfahren, Protokolle, Infrastrukturen. Dpunkt, Heidelberg.
- The Open Web Application Security Project (OWASP) (2005): A guide to building secure web applications and web services. OWASP. (URL: <https://www.um.es/atika/documentos/OWASPGuide2.0.1.pdf> [Retrieved: 11.03.2021]).
- Wätjen, D. (2004): Kryptographie. Grundlagen, Algorithmen, Protokolle. Spektrum Akademischer Verlag, Heidelberg/Berlin.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Seminar
-----------------------------------	---------------------------

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

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

Lehrmethoden	
Lernmaterial <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Prüfungsleitfaden

Kryptologie

Modulcode: DLMCSC_D

Modultyp s. Curriculum	Zugangsvoraussetzungen DLMCSITSDS01	Niveau MA	CP 5	Zeitaufwand Studierende 150 h
----------------------------------	---	---------------------	----------------	---

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

Modulverantwortliche(r)

Prof. Dr. Björn Kaidel (Kryptologie)

Kurse im Modul

- Kryptologie (DLMCSEAITSC02_D)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Fachpräsentation

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Symmetrische und asymmetrische Kryptosysteme
- Authentifizierung
- Kryptoanalyse
- Kryptologie im Internet
- Anwendungen

Qualifikationsziele des Moduls**Kryptologie**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wichtigsten kryptographischen Systeme und Algorithmen und ihre Bedeutung in der heutigen IT zu diskutieren.
- die Sicherheit von internetbasierten Anwendungen zu diskutieren.
- verschiedene kryptographische Systeme und Algorithmen zu bewerten, um eine geeignete Lösung für reale Probleme in der IT auszuwählen.
- Standard-Kryptosysteme und -algorithmen anzuwenden, um reale Probleme in der IT zu lösen.
- bestehende kryptografische Lösungen für reale Probleme zu bewerten und ggf. wesentliche Schwachstellen zu identifizieren.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik

Kryptologie

Kurscode: DLMCSEAITSC02_D

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 5	Zugangsvoraussetzungen DLMCSITSDS01
---------------------	---	------------	----------------	---

Beschreibung des Kurses

Der Schwerpunkt dieses Kurses liegt auf einer umfassenden Einführung in die Kryptologie und ihre wichtigsten Unterpunkte Kryptographie und Kryptoanalyse. Ein besonderes Augenmerk wird auf den Einsatz der Kryptologie zur Unterstützung der Sicherheit von IT-Systemen gelegt. Im ersten Teil des Kurses erhalten die Studenten ein solides Verständnis der grundlegenden Konzepte der Kryptologie, insbesondere symmetrische und asymmetrische Kryptosysteme, Authentifizierung und gängige Ansätze zum Brechen dieser Kryptosysteme mittels Kryptoanalyse. Darauf aufbauend wird die praktische Anwendung der Kryptologie behandelt, beginnend mit einer Einführung in die Standardprotokolle und -techniken, die zur Gewährleistung der Sicherheit der Kommunikation im Internet verwendet werden. Als nächstes werden praktische Aspekte der Anwendung kryptographischer Techniken und Algorithmen behandelt, wie z. B. deren langfristige Sicherheit. Schließlich zeigen einige Anwendungsbeispiele, wie die Konzepte der Kryptologie allgemein verwendet und zur Lösung von Herausforderungen wie Online-Banking eingesetzt werden können.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wichtigsten kryptographischen Systeme und Algorithmen und ihre Bedeutung in der heutigen IT zu diskutieren.
- die Sicherheit von internetbasierten Anwendungen zu diskutieren.
- verschiedene kryptographische Systeme und Algorithmen zu bewerten, um eine geeignete Lösung für reale Probleme in der IT auszuwählen.
- Standard-Kryptosysteme und -algorithmen anzuwenden, um reale Probleme in der IT zu lösen.
- bestehende kryptografische Lösungen für reale Probleme zu bewerten und ggf. wesentliche Schwachstellen zu identifizieren.

Kursinhalt

1. Grundlegende Konzepte der Kryptologie
 - 1.1 Begriffe
 - 1.2 IT-Sicherheit, Bedrohungen und übliche Angriffe
 - 1.3 Historischer Überblick
 - 1.4 Sicherheitskriterien
 - 1.5 Hashfunktionen

2. Symmetrische Kryptosysteme
 - 2.1 Substitution und Transposition
 - 2.2 Blockchiffren
 - 2.3 Digital Encryption Standard (DES)
 - 2.4 Advanced Encryption Standard (AES)
 - 2.5 Kryptografische Hashfunktionen
3. Asymmetrische Kryptosysteme
 - 3.1 Arithmetische Falltüren
 - 3.2 Der Diffie-Hellmann-Schlüsselaustausch
 - 3.3 Der RSA-Algorithmus
 - 3.4 Elliptische Kurven
 - 3.5 Signaturen
 - 3.6 Schlüsselaustausch und Public-Key-Infrastrukturen
4. Authentifizierung
 - 4.1 Passwörter
 - 4.2 Challenge-Response- und Zero-Knowledge-Protokolle
 - 4.3 Biometrische Authentifizierung
 - 4.4 Authentifizierung in verteilten Systemen
 - 4.5 Chipkarten
 - 4.6 Identität und Anonymität
5. Kryptoanalyse – Verschlüsselungen brechen
 - 5.1 Frequenzanalyse
 - 5.2 Brute-Force-Angriffe
 - 5.3 Rainbow Tables
 - 5.4 Bekannte und ausgewählte Klar- und Geheimtexte
 - 5.5 Seitenkanalangriffe
 - 5.6 Moderne kryptoanalytische Algorithmen
6. Kryptologie und das Internet
 - 6.1 Internetprotokolle
 - 6.2 Sicherheit in IP-Netzwerken
 - 6.3 Transport Layer Security
 - 6.4 Sichere E-Mail
 - 6.5 Secure DNS

7. Praktische Aspekte der Kryptologie
 - 7.1 Generierung von Zufallszahlen
 - 7.2 Langfristige Sicherheit
 - 7.3 Kryptographie in der Anwendungsentwicklung
 - 7.4 Rechtliche und regulatorische Aspekte

8. Anwendungen
 - 8.1 Onlinebanking
 - 8.2 Blockchain
 - 8.3 Wahlen
 - 8.4 Steganografie
 - 8.5 Das Tor-Projekt

Literatur

Pflichtliteratur

Weiterführende Literatur

- Esslinger, B. (2010). The CrypTool script: Cryptography, mathematics, and more (10. Aufl.). CrypToolDevelopment Team. (Im Internet verfügbar.)
- Katz, J. & Lindell, Y. (2014). Introduction to modern cryptography (2. Aufl.). Chapman and Hall/ CRC.
- Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. (2001). Handbook of applied cryptography. CRCPress.
- Paar C. & Pelzl J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners.(2. Aufl.). Springer.
- Wätjen D. (2018) Kryptographie: Grundlagen, Algorithmen, Protokolle (3. Aufl.). SpringerFachmedien.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	Online Tests: Ja
Prüfungsleistung	Fachpräsentation

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

Lehrmethoden		
Tutorielle Betreuung <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Lernmaterial <input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Online Tests <input checked="" type="checkbox"/> Prüfungsleitfaden

2. Semester

Cyber Risk Assessment und Management

Modulcode: DLMCSECRAM_D

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

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

Modulverantwortliche(r)

Prof. Dr. Carsten Skerra (Cyber Risk Assessment und Management)

Kurse im Modul

- Cyber Risk Assessment und Management (DLMCSECRAM01_D)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Organisatorisches IT-Risikomanagement
- Messung der Cyber-Bedrohung
- Modellierung von Bedrohungen
- Standardisierung und Konformität
- Risikobewertung
- Die Cyber-resiliente Organisation

Qualifikationsziele des Moduls**Cyber Risk Assessment und Management**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Prozess der Angriffsmodellierung zu verstehen.
- die Auswirkungen eines Angriffes mit den entstehenden Kosten in Verbindung zu bringen.
- sogenannte Black Swan Events zu verstehen.
- den Einfluss des rechtlichen Rahmens auf Risiken und Kosten zu bewerten.
- zu verstehen, wie ein Unternehmen Entscheidungen auf der Grundlage von Risiken treffen muss.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik

Cyber Risk Assessment und Management

Kurscode: DLMCSECRAM01_D

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

Beschreibung des Kurses

Entscheidungen darüber, ob Änderungen vorgenommen werden oder nicht, sollten in Abhängigkeit des Risikos der Auswirkungen eines Einschreitens oder Nicht-Einschreitens getroffen werden. Dies wird neben anderen Faktoren auch von den Kosten bestimmt, die ein potenziell erfolgreicher Angriff verursachen würde. Aber wie kann man Angriffe modellieren und die Kosten mit ihnen in Verbindung bringen? Wir werden uns in diesem Kurs mit der Disziplin der Angriffsmodellierung und Risikobewertung befassen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Prozess der Angriffsmodellierung zu verstehen.
- die Auswirkungen eines Angriffes mit den entstehenden Kosten in Verbindung zu bringen.
- sogenannte Black Swan Events zu verstehen.
- den Einfluss des rechtlichen Rahmens auf Risiken und Kosten zu bewerten.
- zu verstehen, wie ein Unternehmen Entscheidungen auf der Grundlage von Risiken treffen muss.

Kursinhalt

1. Organisatorisches IT-Risikomanagement
 - 1.1 Geschäftlicher Nutzen von Risikomanagement
 - 1.2 Aufbau eines Angriffes zur Exfiltration von Daten
 - 1.3 Cyber-Katastrophen
 - 1.4 Cyber-Risiko
2. Messung der Cyber-Bedrohung
 - 2.1 Messung und Management
 - 2.2 Metriken zur Cyber-Bedrohung
 - 2.3 Messung der Bedrohung für eine Organisation
 - 2.4 Die Eintrittswahrscheinlichkeit schwerwiegender Cyber-Angriffe
 - 2.5 Black-Swan-Events
3. Threat Modeling

- 3.1 Attack-Tree-Methodik
- 3.2 STRIDE
- 3.3 LINDDUN
4. Standardisierung und Compliance
 - 4.1 Das NIST-Risikomanagement-Framework
 - 4.2 ISO/IEC 27005
 - 4.3 BSI-Standard 100-3
5. Risikobewertung
 - 5.1 Methoden
 - 5.2 Berücksichtigung von Black-Swan-Events
 - 5.3 Kontinuierliche Neubewertung
6. Die cyber-resiliente Organisation
 - 6.1 Veränderte Herangehensweisen an das Risikomanagement
 - 6.2 Reaktion auf Zwischenfälle und Krisenmanagement
 - 6.3 Resilience Engineering, Sicherheitslösungen und Finanzen
 - 6.4 Cyber-Versicherung

Literatur

Pflichtliteratur

Weiterführende Literatur

- Antonucci, D. (2017). The cyber risk handbook: Creating and measuring effective cybersecuritycapabilities. Wiley.
- Refsdal, A., Solhaug, B. & Stolen, K. (2015). Cyber-risk management. Springer.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

IT-Systeme: Software

Modulcode: DLMIMITSS

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

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

Modulverantwortliche(r)

Dr. Christian Prause (IT-Systeme: Software)

Kurse im Modul

- IT-Systeme: Software (DLMIMITSS01)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur, 90 Minuten

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Grundlagen der Softwareentwicklung
- Datenformate und Codierung
- Firmware und Betriebssysteme
- Klassifizierung und Anwendungsbereiche von Desktop-Applikationen
- Datenbanken
- Anwendungsspezifische Softwaresysteme im Unternehmen
- Ergonomische Aspekte der Computerarbeitsplatzgestaltung und der Mensch-Maschine-Interaktion

Qualifikationsziele des Moduls**IT-Systeme: Software**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundlagen der Softwareentwicklung zu verstehen.
- Datenformate und ihre Anwendung in unterschiedlichen Szenarien zu beurteilen.
- die Speicherung und Verarbeitung komplexer Daten und Information zu verstehen.
- Betriebssysteme und deren konzeptionelle Unterschiede für Anwendung und Sicherheit zu beurteilen.
- Einsatzgebiete typischer Desktop-Applikationen zu verstehen und deren Grenzen zu beurteilen.
- Datenbank-basierte Unternehmenslösungen zu differenzieren und deren Nutzen für unternehmerische Anwendungsbereiche zu bewerten.
- Anforderungen an Computerarbeitsplätze zu identifizieren und geeignete Lösungen zu implementieren.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik.

IT-Systeme: Software

Kurscode: DLMIMITSS01

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

Beschreibung des Kurses

Der Kurs führt in die Funktion und die Anwendungsbereiche typischer Softwaresysteme ein, die in Unternehmen zum Einsatz kommen. Dazu bilden Konzepte der Softwareentwicklung und der Programmiersprachen die Grundlage. Der Kurs vermittelt notwendige Kenntnisse über Datenformate, deren Konversion, Komprimierung und Transformation, um diese auf die Repräsentation komplexer Daten anzuwenden. Er beschreibt Betriebssysteme für lokale und mobile Computer und deren konzeptionelle Unterschiede und Anwendungsbereiche. Darauf aufbauend werden typische Desktop-Applikationen von Text- bis zur Grafikverarbeitung vorgestellt und deren Einsatzgebiet erläutert. Nach einer Einführung in das Konzept der Datenbanken werden typische Server-basierte Lösungen für das Informationsmanagement behandelt. Der Kurs schließt mit einer Betrachtung ergonomischer Software-Aspekte und der Mensch-Maschine-Interaktion ab.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundlagen der Softwareentwicklung zu verstehen.
- Datenformate und ihre Anwendung in unterschiedlichen Szenarien zu beurteilen.
- die Speicherung und Verarbeitung komplexer Daten und Information zu verstehen.
- Betriebssysteme und deren konzeptionelle Unterschiede für Anwendung und Sicherheit zu beurteilen.
- Einsatzgebiete typischer Desktop-Applikationen zu verstehen und deren Grenzen zu beurteilen.
- Datenbank-basierte Unternehmenslösungen zu differenzieren und deren Nutzen für unternehmerische Anwendungsbereiche zu bewerten.
- Anforderungen an Computerarbeitsplätze zu identifizieren und geeignete Lösungen zu implementieren.

Kursinhalt

1. Grundlagen der Softwareentwicklung
 - 1.1 Grundlagen der Programmierung und Programmiersprachen
 - 1.2 Software-Lebenszyklus
 - 1.3 Software-Lizensierungsmodelle und Patentierung
2. Datenformate

- 2.1 ASCII-Code, Unicode und Auszeichnungssprachen
- 2.2 Seitenbeschreibungssprachen (HTML, XHTML, HTML5)
- 2.3 Scriptsprachen für Webapplikationen
- 2.4 Textformate
- 2.5 Raster-, Vektor-, und Metagrafikformate (PNG, TIFF, JPEG, SVG, WMF)
3. Konversion, Komprimierung und Transformation von Daten
 - 3.1 Datenkonversion (XMI, Transcoding)
 - 3.2 Datenkomprimierung
 - 3.3 Datentransformation
 - 3.4 Anwendung auf audiovisuelle Daten
4. System-Software
 - 4.1 Firmware, BIOS, UEFI
 - 4.2 Betriebssysteme für Endanwender
 - 4.3 Serverbasierte Betriebssysteme
 - 4.4 Mobile Betriebssysteme
5. Desktop-Applikationen
 - 5.1 Office-Software
 - 5.2 Grafik- und Bildbearbeitungsprogramme
 - 5.3 Software für Mathematik und Statistik
 - 5.4 Destop-Publishing und Visualisierung
 - 5.5 Audio- und Videosysteme
6. Datenbanksysteme
 - 6.1 Relationale Datenbanken und SQL
 - 6.2 NoSQL und nicht-relationale Datenbanken
 - 6.3 In-Memory-Datenbanken
 - 6.4 Data Warehousing
7. Business-Systeme
 - 7.1 Webbasierte Systeme und Cloud-Lösungen
 - 7.2 Dokumenten- und Content-Management
 - 7.3 Ressourcenbasiertes Informationsmanagement
 - 7.4 Knowledge-Management, Dashboards und Expertensysteme
8. Ergonomie am Computerarbeitsplatz
 - 8.1 Anthropometrie und Systemergonomie

- 8.2 Produkt- und Produktionsergonomie
- 8.3 Computer-Arbeitsplatzergonomie
- 8.4 Software-Ergonomie
- 8.5 Designaspekte der grafischen Benutzerschnittstelle

Literatur

Pflichtliteratur

Weiterführende Literatur

- Biesel,H./Hame,H. (2018): Vertrieb Und Marketing in Der Digitalen Welt – So Schaffen Unternehmen Die Business Transformation in Der Praxis. Springer Gabler, Wiesbaden.
- Bourke, P./Fairley, R.E. (Hrsg.) (2014): SWEBOK V3.0 –Guide to the Software Engineering Body of Knowledge. IEEE Computer Society.
- Chambers, J.M. (2014): Object-Oriented Programming, Functional Programming and R. Statistical Science. 29. Jg., Heft 2, S.167–180.
- Dankmeier, W. (2017): Grundkurs Codierung. Verschlüsselung, Kompression und Fehlerbeseitigung. 4. Auflage, Springer Vieweg, Wiesbaden.
- Geisler, F. (2014): Datenbanken: Grundlagen und Design. 5. Auflage, MIT Press, Heidelberg.
- Groll, T. (2015): 1x1 des Lizenzmanagements, Praxisleitfaden für Lizenzmanager. 3. Auflage, Hanser Verlag.
- Gumm, H.P./Sommer, M. (2012): Einführung in die Informatik. 10. Auflage, Oldenbourg Verlag, München.
- Meier, A. (2017): Werkzeuge der digitalen Wirtschaft: Big Data, NoSQL & Co. Springer, Wiesbaden.
- Schlick, C./Bruder, R./Luczak, H. (2018): Arbeitswissenschaft. 4. Auflage, Springer, Berlin/ Heidelberg.
- Strutz, T. (2017): Bilddatenkompression. Grundlagen, Codierung, Wavelets, JPEG, MPEG, H.264, HVEC. 4. Auflage, Springer Vieweg, Wiesbaden.
- Tanenbaum, A.S./Bos, H. (2016): Moderne Betriebssysteme.4. Auflage, Pearson Deutschland, Hallbergmoos.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

IT-Systeme: Hardware

Modulcode: DLMIMITSH

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

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

Modulverantwortliche(r)

Prof. Dr. Markus C. Hemmer (IT-Systeme: Hardware)

Kurse im Modul

- IT-Systeme: Hardware (DLMIMITSH01)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur, 90 Minuten

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Rechnerarithmetik
- Integrierte Schaltkreise
- Speichersysteme
- Ein-/Ausgabesysteme
- Grundlagen der Datenübertragung
- Computernetze
- Server und Rechenzentren

Qualifikationsziele des Moduls**IT-Systeme: Hardware**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Rechnerarithmetik zu verstehen und auf logische Problemstellungen anzuwenden.
- Bestandteile von Rechner-Systemen zu kennen und deren Funktionsprinzipien zu erklären.
- Methoden der Datenübertragung zu differenzieren und deren konzeptionelle Unterschiede in der Anwendung zu bewerten.
- Computernetztechnologien und deren Einsatzgebiete zu beurteilen.
- Anforderungen für den Aufbau und den Betrieb von Rechenzentren zu kennen und zu beurteilen.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik.

IT-Systeme: Hardware

Kurscode: DLMIMITSH01

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

Beschreibung des Kurses

Der Kurs vermittelt das Verständnis der Funktionsweise computerbasierter Systeme und dient als Basis für die Kommunikation und Führung entsprechender Fachkräfte der Informationstechnologie. Er beschreibt die Logik, mit der digitale Computer arbeiten und die Technik der Herstellung digitaler Schaltkreise. Weiterhin erläutert er den Aufbau typischer Computersysteme und die Funktionsweise von Prozessoren, Speicherbausteinen und peripherer Ein- und Ausgabegeräte. Er vermittelt die Grundlagen der Nachrichtentechnik und stellt die Einsatzkriterien kabelgebundener und kabelloser Datenübertragungstechniken gegenüber. Auf dieser Grundlage werden kleine Server-Infrastrukturen, Großrechner und Supercomputer vorgestellt und Kenntnisse zum Aufbau und Betrieb von Rechenzentren vermittelt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Rechnerarithmetik zu verstehen und auf logische Problemstellungen anzuwenden.
- Bestandteile von Rechner-Systemen zu kennen und deren Funktionsprinzipien zu erklären.
- Methoden der Datenübertragung zu differenzieren und deren konzeptionelle Unterschiede in der Anwendung zu bewerten.
- Computernetztechnologien und deren Einsatzgebiete zu beurteilen.
- Anforderungen für den Aufbau und den Betrieb von Rechenzentren zu kennen und zu beurteilen.

Kursinhalt

1. Grundlagen der Rechnerarithmetik
 - 1.1 Stellenwertarithmetik, Zahlensysteme
 - 1.2 Aussagenlogik und boolesche Operatoren
 - 1.3 Rechnerarithmetik
2. Integrierte Schaltkreise
 - 2.1 Integrierte Schaltkreise und Halbleiterproduktion
 - 2.2 Parallele und serielle Schnittstellen
 - 2.3 Komponenten der Hauptplatine
 - 2.4 Prozessoren und Speicher

3. Speichersysteme
 - 3.1 Festplattenspeicher
 - 3.2 Optische Speichermedien
 - 3.3 Magnetische Wechseldatenträger
 - 3.4 Solid State Disk
4. Ein-/Ausgabesysteme
 - 4.1 Eingabegeräte
 - 4.2 Sensorbildschirmssysteme
 - 4.3 Bildausgabegeräte
 - 4.4 Druckersysteme
5. Grundlagen der Datenübertragung
 - 5.1 Kabelgebundene Datenübertragung und Modulation
 - 5.2 Übertragung mittels Licht
 - 5.3 Antennen und Satellitentechnik
 - 5.4 Mobilfunknetze
 - 5.5 RFID und Near-Field Communication
6. Computernetze
 - 6.1 Netzwerk-Topologie
 - 6.2 Ethernet-Frame und Netzwerkprotokolle
 - 6.3 Switching, Routing und Datenflusssteuerung
 - 6.4 Netzwerkdiagnose
7. Server und Rechenzentren
 - 7.1 Multi-Tier-Architekturen
 - 7.2 Server-Systeme, Großrechner und Supercomputer
 - 7.3 Aufbau von Rechenzentren
 - 7.4 Aspekte der Sicherheit und des Betriebs von Rechenzentren
 - 7.5 Prinzipien der Virtualisierung

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

- Beetz, J. (2019): Digital – Wie Computer denken. Springer, Berlin.
- Dürr, B. (2018): IT-Räume und Rechenzentren planen und betreiben: Handbuch der Bautechnik und Technischen Gebäudeausrüstung. Verlag Bau+Technik, Erkrath.
- Geng, H. (2015): Data Center Handbook. Wiley, New York.
- Hoffmann, D.W. (2016): Grundlagen der Technischen Informatik. Carl Hanser Verlag, München.
- Schiffmann, W./Bähring, H./Hönig, U. (2011): Technische Informatik 3 - Grundlagen der PC-Technologie. Springer, Berlin.
- Tanenbaum, A. S./Wetherall, D. J. (2012): Computernetzwerke. Pearson, München.
- Werner, M. (2017): Nachrichtentechnik: Eine Einführung für alle Studiengänge. Springer Vieweg, Wiesbaden.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

Cybersysteme und Netzwerkforensik

Modulcode: DLMCSECSNF_D

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

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

Modulverantwortliche(r)

Petra Beenken (Cybersysteme und Netzwerkforensik)

Kurse im Modul

- Cybersysteme und Netzwerkforensik (DLMCSECSNF01_D)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Betriebssysteme
- Vernetzung
- Forensik
- Kryptographie
- Cyber-Angriffe

Qualifikationsziele des Moduls**Cybersysteme und Netzwerkforensik**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende interne Strukturen, Aufbau und Funktionen von Betriebssystemen zu verstehen.
- die wichtigsten Netzwerkprotokolle zu verstehen.
- Angriffe auf Computer und Netzwerke zu diagnostizieren
- die Wichtigkeit der Beweiserhebung und Beweissicherung zu verstehen.
- wesentliche Angriffsmuster zu verstehen.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik

Cybersysteme und Netzwerkforensik

Kurscode: DLMCSECSNF01_D

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

Beschreibung des Kurses

Der Computersicherheitsexperte hat die schwierige Aufgabe, sowohl die Grundlagen von Betriebssystemen als auch von Netzwerken kennen zu müssen. In diesem Kurs betrachten wir Betriebssysteme und Netzwerke aus forensischer Sicht. Das Endergebnis ist das Verständnis von Angriffen auf eine Organisation.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende interne Strukturen, Aufbau und Funktionen von Betriebssystemen zu verstehen.
- die wichtigsten Netzwerkprotokolle zu verstehen.
- Angriffe auf Computer und Netzwerke zu diagnostizieren
- die Wichtigkeit der Beweiserhebung und Beweissicherung zu verstehen.
- wesentliche Angriffsmuster zu verstehen.

Kursinhalt

1. Betriebssysteme
 - 1.1 Konzepte
 - 1.2 Speicherverwaltung
 - 1.3 Prozess-Management
 - 1.4 Geräteverwaltung
 - 1.5 Eingabe/Ausgabe
2. Betriebssystembausteine
 - 2.1 Systemaufrufe
 - 2.2 Prozesstabellen-Analyse
 - 2.3 Windows-Registrierungsdatenbank
 - 2.4 Dateisystem-Forensik
 - 2.5 Typische Angriffe
3. Der Netzwerkstapel
 - 3.1 TCP/IP- und OSI-Netzwerkstapel

- 3.2 Zentrale Internet-Dienste
- 3.3 Das World Wide Web
- 3.4 Transportschicht-Verschlüsselung
- 3.5 Typische Angriffe
4. Computer-Forensik
 - 4.1 Beweisführung
 - 4.2 Schadsoftware
 - 4.3 Daten-Exfiltration
 - 4.4 Angriffe gegen Computer-Forensik
5. Netzwerk-Forensik
 - 5.1 Indikatoren für eine Kompromittierung
 - 5.2 Einbindung externer Daten (Datenanreicherung) und Entscheidungspunkte
 - 5.3 Angriffe gegen die Netzwerk-Forensik
6. Angriffe aus der Sicht des Zentralrechners und des Netzwerks
 - 6.1 Techniken, Taktiken und Verfahren
 - 6.2 Erkennung und Verhinderung von Eindringversuchen
 - 6.3 Korrelation von Ereignissen

Literatur

Pflichtliteratur

Weiterführende Literatur

- Kaufman C. / Perlman, R. / Speciner, M. (2002): Network Security: Private Communication in a Public World, Second Edition, Pearson Education, London.
- Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.
- Pfleeger C. P. / Pfleeger S. L. / Margulies, J. (2015): Security in Computing. 5th Edition, Pearson Education, London.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

Netzwerksicherheit

Modulcode: DLMCSEESN1_D

Modultyp s. Curriculum	Zugangsvoraussetzungen DLMIMITSS01_E oder DLMIMITSS01; DLMIMITSH01_E oder DLMIMITSH01	Niveau MA	CP 5	Zeitaufwand Studierende 150 h
----------------------------------	--	---------------------	----------------	---

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

Modulverantwortliche(r)

Prof. Dr. Björn Kaidel (Netzwerksicherheit)

Kurse im Modul

- Netzwerksicherheit (DLMCSEESN01_D)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Kryptographische Protokolle
- Netzwerksicherheitsmaßnahmen
- Sicherheitsprobleme auf der Anwendungsebene
- Drahtlose Sicherheit
- Einbruchserkennung und -prävention

Qualifikationsziele des Moduls**Netzwerksicherheit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die in Netzwerken verwendete Kryptographie zu verstehen.
- zu verstehen, was Identitäten sind und wie Authentifizierung funktioniert.
- mit verschiedenen Netzwerksicherheitsprotokollen zu arbeiten.
- die Zugriffskontrollen für Netzwerke einzurichten.
- die Konzepte für die Cloud-Sicherheit zu verstehen.
- die Einbruchserkennung einzusetzen.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik

Netzwerksicherheit

Kurscode: DLMCSEESN01_D

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 5	Zugangsvoraussetzungen DLMIMITSS01_E oder DLMIMITSS01; DLMIMITSH01_E oder DLMIMITSH01
---------------------	---	------------	----------------	--

Beschreibung des Kurses

Systeme sind intern untereinander vernetzt und kommunizieren auch über das Internet. Die allgemeine Aufgabe der Netzwerksicherheit besteht darin, Vertraulichkeit, Integrität, Nachweisbarkeit und Verfügbarkeit von Daten zu gewährleisten, die in Netzwerken übertragen oder in vernetzten Systemen gespeichert werden.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die in Netzwerken verwendete Kryptographie zu verstehen.
- zu verstehen, was Identitäten sind und wie Authentifizierung funktioniert.
- mit verschiedenen Netzwerksicherheitsprotokollen zu arbeiten.
- die Zugriffskontrollen für Netzwerke einzurichten.
- die Konzepte für die Cloud-Sicherheit zu verstehen.
- die Einbruchserkennung einzusetzen.

Kursinhalt

1. Überblick über die Netzwerksicherheit
 - 1.1 ISO/OSI- und TCP/IP-Modell
 - 1.2 Angriffe und Gegenmaßnahmen
 - 1.3 Netzwerktopologien
 - 1.4 Grundlegende Sicherheitsmodelle
2. Infrastrukturelle Komponenten
 - 2.1 Firewalls
 - 2.2 Routing ACLs
 - 2.3 Switches
 - 2.4 Angriffe in Verbindung mit Routern, Switches und Firewalls
3. Kryptographie
 - 3.1 Symmetrische Kryptographie
 - 3.2 Asymmetrische Kryptographie und Schlüsselverwaltung

- 3.3 Kryptographische Hash-Funktion
- 3.4 Quantenresistente Verschlüsselung und Quantenschlüsselaustausch
- 4. Authentifizierung
 - 4.1 Identität
 - 4.2 System- und Benutzerauthentifizierung
 - 4.3 Datenauthentifizierung
 - 4.4 Multi-Faktor-Authentifizierung
- 5. Sicherheitsprotokolle
 - 5.1 Public-Key-Infrastruktur
 - 5.2 IPsec - Network Layer Security Protocol
 - 5.3 TLS - Transport Layer Security Protocol
 - 5.4 Kerberos - Authentifizierungsprotokoll
 - 5.5 SSH - Sicherheitsprotokoll für Fernanmeldung
 - 5.6 PGP und S/MIME - E-Mail-Sicherheitsprotokoll
- 6. Sicherheit im drahtlosen Netzwerk
 - 6.1 Wi-Fi Protected Access
 - 6.2 WPA2/IEEE 802.11i
 - 6.3 Sicherheit in Bluetooth
 - 6.4 Sicherheit in ZigBee
- 7. Cloud-Sicherheit
 - 7.1 Cloud-Service-Modelle
 - 7.2 Cloud-Sicherheitsmodelle
 - 7.3 Mehrere Tenants
 - 7.4 Suchen in verschlüsselten Daten
- 8. Einbruchserkennung und -prävention
 - 8.1 Grundlegende Konzepte
 - 8.2 Netzwerk- und Host-basierte Erkennungen
 - 8.3 Signaturbasierter Ansatz
 - 8.4 Verhaltensbasierter Ansatz

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

- Bullock, J., & Parker, J. (2017). Wireshark for security professionals: Using wireshark and the metasploit framework. John Wiley & Sons.
- Monte, M. (2015). Network attacks and exploitation: A framework. John Wiley & Sons.
- Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer.
- Schneier, B. (2015). Applied cryptography: Protocols, algorithms and source code in C. (20th anniversary ed.). John Wiley & Sons.
- Wack, J. P. (2002). Guidelines on firewalls and firewall policy. National Institute of Standards and Technology.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Musterklausur <input checked="" type="checkbox"/> Online Tests

Theoretische Informatik für IT-Sicherheit

Modulcode: DLMCSETCSITS_D

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

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

Modulverantwortliche(r)

Prof. Dr. Björn Kaidel (Theoretische Informatik für IT-Sicherheit)

Kurse im Modul

- Theoretische Informatik für IT-Sicherheit (DLMCSETCSITS01_D)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Algorithmen und Datenstrukturen
- Formale Sprachen und Automatentheorie
- Berechenbarkeit, Entscheidbarkeit und Komplexität
- Logik
- Algorithmus- und Programmverifizierung
- Künstliche Intelligenz und Maschinelles Lernen

Qualifikationsziele des Moduls**Theoretische Informatik für IT-Sicherheit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grenzen von Datenstrukturen, Algorithmen und Berechnungen im Allgemeinen zu verstehen.
- formale Sprachen und Automaten zur Lösung von Sicherheitsproblemen einzusetzen.
- Techniken des maschinellen Lernens bei der Datenanalyse einzusetzen.
- Logik und Wissensrepräsentation zu verwenden.
- die Prinzipien der Programmanalyse und -überprüfung zu verstehen.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik

Theoretische Informatik für IT-Sicherheit

Kurscode: DLMCSETCSITS01_D

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

Beschreibung des Kurses

In der Praxis der IT-Sicherheit stoßen wir oft an die Grenzen der Informationstechnik und der Informatik. Was manchmal so aussieht, als sollte es lösbar sein, erweist sich für heutige Computer als schwierig oder unmöglich. Die Theoretische Informatik liefert den Rahmen für das Verständnis schwieriger Probleme und bietet oft einen Weg zu anderen Lösungen. Hier kann maschinelles Lernen oft eine stochastische Lösung bieten, wo es keine genaue gibt. Wir behandeln in diesem Kurs auch das Thema Programmanalyse und -verifikation.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grenzen von Datenstrukturen, Algorithmen und Berechnungen im Allgemeinen zu verstehen.
- formale Sprachen und Automaten zur Lösung von Sicherheitsproblemen einzusetzen.
- Techniken des maschinellen Lernens bei der Datenanalyse einzusetzen.
- Logik und Wissensrepräsentation zu verwenden.
- die Prinzipien der Programmanalyse und -überprüfung zu verstehen.

Kursinhalt

1. Algorithmen und Datenstrukturen
 - 1.1 Algorithmen, Programmiersprachen und Datenstrukturen
 - 1.2 Graphen und Bäume
 - 1.3 Sortieren und Suche
 - 1.4 Analyse von Algorithmen
2. Formale Sprachen und Automatentheorie
 - 2.1 Sprachen und Grammatiken
 - 2.2 Reguläre Sprachen und endliche Automaten
 - 2.3 Kontextfreie Sprachen und Kellerautomaten
 - 2.4 Kontextsensitive Sprachen und Turingmaschinen
3. Berechenbarkeit, Entscheidbarkeit und Komplexität
 - 3.1 Berechenbarkeit

- 3.2 Entscheidbarkeit und Entscheidungsprobleme
- 3.3 Komplexitätstheorie
- 3.4 Quantencomputing
- 4. Logik
 - 4.1 Aussagenlogik
 - 4.2 Prädikatenlogik
 - 4.3 Resolutionskalkül
 - 4.4 Tableauekalkül
- 5. Algorithmus- und Programmverifizierung
 - 5.1 Programmanalyse
 - 5.2 Algebraische, operationale und denotationale Semantik
 - 5.3 Abstrakte Interpretation
- 6. Künstliche Intelligenz und Maschinelles Lernen
 - 6.1 Überwachtes vs. unüberwachtes Lernen
 - 6.2 Lineare und nichtlineare Regression
 - 6.3 Logistische Regression
 - 6.4 Künstliche Neuronale Netze

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

- Goodfellow, I. / Bengio, Y. / Courville, A. (2016): Deep Learning. MIT Press, Cambridge, MA.
- Graham, R. L. / Knuth, D. E. / Patashnik, O. (1994): Concrete Mathematics. A Foundation for Computer Science. 2nd Edition, Addison-Wesley, Upper Saddle River, NJ.
- Hoffmann, D. W. (2018): Theoretische Informatik. 4., aktualisierte Auflage, Carl Hanser Verlag GmbH & Co. KG, München.
- Hopcroft, J. E. / Ullman J. D. (2006): Introduction to Automata Theory, Languages, and Computation. 3rd Edition, Pearson Education, London.
- Kastens, U./Kleine Büning, H. (2018): Modellierung. Grundlagen und formale Methoden. 4., erweiterte Auflage. Carl Hanser Verlag GmbH & Co. KG, München.
- Krumke, S. O./Noltemeier, H. (2012): Graphentheoretische Konzepte und Algorithmen. 3. Auflage, Vieweg+Teubner Verlag, Wiesbaden.
- Nielson, F. / Nielson, H. R. / Hankin, C. (1999): Principles of Program Analysis. Springer, Berlin.
- Nipkow T. / Klein, G. (2016): Concrete Semantics. With Isabelle/HOL. Springer, Berlin.
- Russell, S. / Norvig, P. (2016): Artificial Intelligence. A Modern Approach. Pearson Education, London.
- Shaffer, C. A. (2011): Data Structures and Algorithm Analysis in C++. 3rd Edition, Dover Books on Computer Science, Mineola, NY.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

3. Semester

Seminar: Standards und Frameworks

Modulcode: DLMIMSSF

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

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

Modulverantwortliche(r)

Prof. Dr. André Köhler (Seminar: Standards und Frameworks)

Kurse im Modul

- Seminar: Standards und Frameworks (DLMIMSSF01)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Schriftliche Ausarbeitung: Seminararbeit

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Das Seminar stellt eine Methodik vor, um Prinzipien von Standards und Rahmenwerken zu hinterfragen, explizite und implizite Annahmen zu identifizieren und zu validieren und empfohlene Kategorisierungen und Arbeitsabläufe hinsichtlich ihrer Umsetzbarkeit zu bewerten.

Qualifikationsziele des Moduls**Seminar: Standards und Frameworks**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-relevante Standards und Frameworks zu benennen und anhand derer Einsatzgebiete abzugrenzen.
- Prinzipien der Standards und Frameworks auf ihre Umsetzbarkeit und logische Argumentation hin zu hinterfragen.
- gemachte Annahmen in Standards zu identifizieren und zu validieren.
- empfohlene Kategorisierungen und Arbeitsabläufe auf ihre Plausibilität hin zu überprüfen.
- administrative und technische Voraussetzungen für die Implementierung zu identifizieren.
- Erwartungen der Stakeholder zu identifizieren und zu priorisieren.
- Empfehlungen zur Umsetzung und Erhaltung der Standards zu geben.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik

Seminar: Standards und Frameworks

Kurscode: DLMIMSSF01

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

Beschreibung des Kurses

Das Seminar macht Studierende mit einer Vorgehensweise zur kritischen Beurteilung internationaler Standards und Rahmenwerke der IT vertraut. Studierende werden damit in die Lage versetzt, in einem gegebenen Industrieszenario die Nutzbarkeit und Grenzen eines Standards einzuschätzen und Entscheidungsträgern entsprechende Empfehlungen zu geben. Das Seminar fokussiert dabei auf die kritische Beurteilung der Prinzipien und Annahmen der Standards, der Konsistenz und Kohärenz empfohlener Kategorien und Arbeitsanweisungen und der Einschätzung der Umsetzbarkeit, Implementierung und Erhaltung des Standards. Auf dieser Basis erstellen die Studierenden für einen gegebenen Standard in einem gegebenen Industrieszenario einen Bericht, der den Standard entsprechend dieser Kriterien bewertet und mit einer Empfehlung zur Befürwortung oder Ablehnung des Standards abschließt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-relevante Standards und Frameworks zu benennen und anhand derer Einsatzgebiete abzugrenzen.
- Prinzipien der Standards und Frameworks auf ihre Umsetzbarkeit und logische Argumentation hin zu hinterfragen.
- gemachte Annahmen in Standards zu identifizieren und zu validieren.
- empfohlene Kategorisierungen und Arbeitsabläufe auf ihre Plausibilität hin zu überprüfen.
- administrative und technische Voraussetzungen für die Implementierung zu identifizieren.
- Erwartungen der Stakeholder zu identifizieren und zu priorisieren.
- Empfehlungen zur Umsetzung und Erhaltung der Standards zu geben.

Kursinhalt

- Die Analyse beginnt mit der Bewertung der Ähnlichkeiten und Unterschiede bezüglich der Einsatzgebiete der Standards. Darauf folgt eine Einschätzung der Intention der Herausgeber, der Popularität des Standards sowie der Begründung der Einführung in ausgewählten Industriesektoren. Auf dieser Basis erstellen die Studierenden eine Seminararbeit, in der sie für einen gegebenen Standard in einem gegebenen Industrieszenario eine kritische Einschätzung der Umsetzbarkeit vornehmen. Die Seminararbeit deckt dabei folgende Kriterien ab:
 - Prinzipien: Eine kritische Bewertung der Prinzipien des Standards für das gegebene Industrieszenario.

- Annahmen: Identifizierung der im Standard gemachten expliziten und impliziten Annahmen und deren Plausibilitätsprüfung im gegebenen Industrieszenario.
- Kategorien: Bewertung der Übereinstimmung der vorgegebenen Kategorisierungen mit dem Industrieszenario.
- Abläufe: Ermittlung der notwendigen Arbeitsabläufe und Einschätzung der Machbarkeit.
- Erwartungen: Identifizierung der Anforderungen und Erwartungen der Stakeholder.
- Konsistenzprüfung: Identifizierung von Widersprüchen in einer der vorgenannten Kategorien.
- Kohärenzprüfung: Bewertung der Vollständigkeit und ggf. Empfehlungen für weitere Standardisierung.
- Voraussetzungen: Ermittlung der Voraussetzungen zur Implementierung des Standards.
- Aufrechterhaltung: Eine Einschätzung des Aufwands zur Erhaltung und Pflege des Standards.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Johannsen, W./Goeken, M. (2011): Referenzmodelle für IT-Governance. Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co. dpunkt.verlag, Heidelberg.
- Krallmann, H./Bobrik, A./Levina, O. (Hrsg.) (2013): Systemanalyse im Unternehmen. Prozessorientierte Methoden der Wirtschaftsinformatik. Walter de Gruyter, Berlin.
- Müller, K. R. (2018): IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement–Sichere Anwendungen–Standards und Practices. Springer, Berlin.
- Rüter, A. et al. (Hrsg.) (2010): IT-Governance in der Praxis. Erfolgreiche Positionierung der IT im Unternehmen. Anleitung zur erfolgreichen Umsetzung regulatorischer und wettbewerbsbedingter Anforderungen. Springer, Berlin.
- Tiemeyer, E. (Hrsg.) (2016): Handbuch IT-Systemmanagement. Handlungsfelder, Prozesse, Managementinstrumente, Good-Practices. Carl Hanser Verlag, München.
- van Wessel, R. (Hrsg.) (2010): Toward Corporate IT Standardization Management. Frameworks and Solutions. IGI Global, Hershey, PA.
- Wagner, K. P. (2015): Ermittlung des Reifegrads von Informationstechnologie in kleinen und mittleren Unternehmen. Berliner Wissenschaftsverlag, Berlin.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Seminar
-----------------------------------	---------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Lernmaterial <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Prüfungsleitfaden

Projekt: Aktuelle Herausforderungen der Cyber-Sicherheit

Modulcode: DLMCSEPCCCS_D

Modultyp s. Curriculum	Zugangsvoraussetzungen DLMCSITSDS01 oder DLMCSITSDP01	Niveau MA	CP 5	Zeitaufwand Studierende 150 h
----------------------------------	--	---------------------	----------------	---

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

Modulverantwortliche(r)

Prof. Dr. Jörn-Marc Schmidt (Projekt: Aktuelle Herausforderungen der Cyber-Sicherheit)

Kurse im Modul

- Projekt: Aktuelle Herausforderungen der Cyber-Sicherheit (DLMCSEPCCCS01_D)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Schriftliche Ausarbeitung: Projektbericht

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Die Computersicherheit entwickelt sich ständig weiter. Dieser Kurs gibt den Studierenden die Möglichkeit sich mit dem neuesten Stand der Sicherheitsforschung und der Sicherheitspraxis auseinanderzusetzen, indem Studierende ihr Wissen auf ein aktuelles Problem in diesem Bereich anwenden.

Qualifikationsziele des Moduls**Projekt: Aktuelle Herausforderungen der Cyber-Sicherheit**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ein Projekt auf dem Gebiet der Computersicherheit abzuschließen, das einen Forschungsaspekt beinhaltet.
- die Computersicherheit über den etablierten Stand der Technik hinaus zu erforschen.
- einen Bericht zu schreiben, der den Beitrag der Studierenden zur interdisziplinären Forschung im Bereich der Computersicherheit hervorhebt.
- zum Stand der Technik in der Computersicherheit beizutragen.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik

Projekt: Aktuelle Herausforderungen der Cyber-Sicherheit

Kurscode: DLMCSEPCCCS01_D

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 5	Zugangsvoraussetzungen DLMCSITSDS01 oder DLMCSITSDP01
---------------------	---	------------	----------------	--

Beschreibung des Kurses

Die Computersicherheit entwickelt sich ständig weiter. In diesem Projekt haben Studierende die Möglichkeit, zur interdisziplinären Forschung der Computersicherheit beizutragen, indem sie ihr Wissen auf ein aktuelles Thema der Informatik anwenden, das einen umfassenden, neuartigen Ansatz der Computersicherheit erfordert. Themen können die Analyse einer speziellen Bedrohung, ein Bericht und die Analyse einer neuen Sicherheitstechnologie, die Implementierung einer Sicherheitslösung oder ein Projekt sein, das speziell die bewährten Sicherheitspraktiken (best practices) anwendet, usw. Auf diese Weise können die Studierenden ihre Fähigkeiten im Bereich der Computersicherheit unter Beweis stellen und sich auf die Masterarbeit vorbereiten.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ein Projekt auf dem Gebiet der Computersicherheit abzuschließen, das einen Forschungsaspekt beinhaltet.
- die Computersicherheit über den etablierten Stand der Technik hinaus zu erforschen.
- einen Bericht zu schreiben, der den Beitrag der Studierenden zur interdisziplinären Forschung im Bereich der Computersicherheit hervorhebt.
- zum Stand der Technik in der Computersicherheit beizutragen.

Kursinhalt

- Der Studierende recherchiert ein Thema, entwickelt eine entsprechende Lösung zu einem gegebenen Problem und/oder einem gegebenen Kontext und reicht dann den Bericht und falls angemessenen entwickelten CODE und spezifische 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>
- Falliere, N. / O Murchu, L. / Chien, E. (2010): W32.Stuxnet Dossier. Symantec, Tempe, AZ. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
- Hacquebord, F. (2020): Pawn Storm in 2019 A Year of Scanning and Credential Phishing on High-Profile Targets. Trend Micro Research, Irving, TX. https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf
- Vulnerability Notes Database: <https://www.kb.cert.org/vuls/>

Studienformat Fernstudium

Studienform Fernstudium	Kursart Projekt
-----------------------------------	---------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Lernmaterial <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Prüfungsleitfaden

Computerkriminalität

Modulcode: DLMIMWCK

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

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

Modulverantwortliche(r)

Prof. Dr. Alexander Lawall (Angriffsszenarien und Vorfallreaktion) / Prof. Dr. Alexander Lawall (Projekt: Cyber-Forensik)

Kurse im Modul

- Angriffsszenarien und Vorfallreaktion (DLMIMWCK01)
- Projekt: Cyber-Forensik (DLMIMWCK02)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Angriffsszenarien und Vorfallreaktion

- Studienformat "Fernstudium": Klausur, 90 Minuten

Projekt: Cyber-Forensik

- Studienformat "Fernstudium": Portfolio

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Angriffsszenarien und Vorfallreaktion

- Bedrohungsszenarien
- Angriffsvektoren
- Präventive Maßnahmen
- Reaktive Maßnahmen
- Aktuelle Lage der IT-Sicherheit

Projekt: Cyber-Forensik

Das Projekt befasst sich mit der Frage, welche Vorgehensweise geeignet ist, um auf computerkriminelle Vorfälle im Unternehmen reagieren zu können. Es behandelt forensische Verfahren zur Erfassung gerichtsverwertbarer Beweise sowie Empfehlungen zur Risikominimierung, zur Kommunikation und zur Prävention solcher Vorfälle.

Qualifikationsziele des Moduls

Angriffsszenarien und Vorfallreaktion

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Bedrohungsszenarien und deren Auswirkungen zu bewerten.
- Angriffsvektoren zu benennen und adäquate Gegenmaßnahmen auszuwählen.
- Verfahren der elektronischen Beweisführung auf gewählte Angriffsszenarien anzuwenden.
- präventive Maßnahmen zu erarbeiten.
- reaktive Maßnahmen zu benennen und deren Wirksamkeit zu bewerten.
- Information zur aktuellen Bedrohungssituation zu sammeln und auszuwerten.

Projekt: Cyber-Forensik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Methoden und Techniken der Computerforensik und deren Limitationen zu benennen.
- die von einer computerkriminellen Handlung betroffenen Systeme und Geschäftsprozesse zu identifizieren und eine Risikoabschätzung vorzunehmen.
- Maßnahmen zur Sicherstellung elektronischer Beweise zu empfehlen und deren Gerichtsverwertbarkeit zu evaluieren.
- Empfehlungen zur Vorfall-Kommunikation, -Reaktion und -Prävention zu entwickeln.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik

Angriffsszenarien und Vorfallreaktion

Kurscode: DLMIMWCK01

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

Beschreibung des Kurses

Der Kurs vermittelt Studierenden Kenntnisse zur Identifizierung und Maßnahmenplanung im Umgang mit kriminellen Angriffen im digitalen Umfeld. Er beschreibt, wie Schwachstellen in Hardware und Software sowie in deren Anwendung für kriminelle Aktivitäten ausgenutzt werden können. Dazu werden typische Bedrohungsszenarien vorgestellt und die Wege, auf denen angreifende Systeme in ein Computersystem eindringen können. Der Kurs führt zudem in Methoden der elektronischen Beweisführung ein und zeigt, wie im Angriffsfall rechtlich verwertbare Informationen gewonnen werden können. Im Anschluss werden die Entwicklung präventiver Maßnahmen und die Reaktionsmöglichkeiten im konkreten Bedrohungsfall erörtert. Der Kurs behandelt abschließend, wie aus Berichten der Sicherheitsbehörden (wie etwa BSI, Europol, NCA, FBI) Informationen zur aktuellen Sicherheitslage gewonnen werden können.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Bedrohungsszenarien und deren Auswirkungen zu bewerten.
- Angriffsvektoren zu benennen und adäquate Gegenmaßnahmen auszuwählen.
- Verfahren der elektronischen Beweisführung auf gewählte Angriffsszenarien anzuwenden.
- präventive Maßnahmen zu erarbeiten.
- reaktive Maßnahmen zu benennen und deren Wirksamkeit zu bewerten.
- Information zur aktuellen Bedrohungssituation zu sammeln und auszuwerten.

Kursinhalt

1. Einführung
 - 1.1 Computerkriminalität in Abgrenzung zu anderen Angriffen
 - 1.2 Schwachstellen in Computer und Mobilgeräten
 - 1.3 Eine Übersicht über Schadsoftware
 - 1.4 Social Engineering und der menschliche Faktor
2. Strafrechtliche Basis
 - 2.1 Identitätsmissbrauch
 - 2.2 Diebstahl von geistigem Eigentum
 - 2.3 Fälschung beweisrelevanter Daten
 - 2.4 Computerbetrug

3. Spezifische Delikte
 - 3.1 Datendiebstahl
 - 3.2 Digitale Erpressung
 - 3.3 Computersabotage
 - 3.4 Industriespionage
4. Angriffsvektoren
 - 4.1 Angriffe auf Chip- und Firmware-Ebene
 - 4.2 Angriffe auf Betriebssystemebene
 - 4.3 Angriffe auf Netzwerk- und Serverebene
 - 4.4 Angriffe auf Anwendungsebene
 - 4.5 Angriffe auf Organisationsebene
5. IT-Forensik und elektronische Beweisführung
 - 5.1 Identifizierung, Lokalisierung und der Umgang mit Polymorphismen
 - 5.2 Mechanismen zur Angriffserkennung
 - 5.3 Auffinden elektronischer Beweise
 - 5.4 Wiederherstellung von Daten und Beweisrückgewinnung
 - 5.5 Rechtliche Grenzen und prädiktive Methoden
6. Präventive Maßnahmen
 - 6.1 Maßnahmen auf Hardware-Ebene
 - 6.2 Zugangsberechtigung, Autorisierung und Authentifizierung
 - 6.3 Sensibilisierung & Schulung
 - 6.4 Vorfallreaktionsplanung
7. Reaktive Maßnahmen
 - 7.1 Erstbeurteilung und Schadensausmaß
 - 7.2 Unterbindung anhaltender Schäden
 - 7.3 Sammlung, Austausch und Verteilung von Information
 - 7.4 Zusammenarbeit mit Sicherheitsbehörden und Kooperationspartnern
 - 7.5 Handlungsempfehlungen für Unternehmen
8. Die aktuelle Sicherheitslage
 - 8.1 Aktuelle Berichte der Sicherheitsbehörden
 - 8.2 Bewertung der Empfehlungen der Sicherheitsbehörden
 - 8.3 Aktuelle Themen der Europol Awareness Campaign

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

- Fleischer, D. (2016): Wirtschaftsspionage. Springer Fachmedien, Wiesbaden.
- Klipper, S. (2015): Cyber Security. Ein Einblick für Wirtschaftswissenschaftler. Springer, Berlin.
- Kraft, P./Weyert, A. (2017): Network Hacking. Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe. Franzis Verlag, München.
- Labudde, D./Spranger, M. (Hrsg.) (2017): Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. Springer, Berlin.
- Lenhard, T. H. (2017): Datensicherheit. Technische und organisatorische Schutzmassnahmen gegen Datenverlust und Computerkriminalität. Springer, Berlin.
- Lewis, J./Baker, S. (2013): The economic impact of cybercrime and cyber espionage. McAfee, Santa Clara, CA.
- Müller, K. R. (2018): IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement–Sichere Anwendungen–Standards und Practices. Springer, München.
- Yar, M./Steinmetz, K. F. (2019): Cybercrime and society. SAGE Publications, Thousand Oaks, CA.
- Hyperlinks zu aktuellen Berichten und Empfehlungen von Sicherheitsbehörden und Institutionen (z.B. BSI, Europol, FBI) werden im Kurs zur Verfügung gestellt.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

Projekt: Cyber-Forensik

Kurscode: DLMIMWCK02

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 5	Zugangsvoraussetzungen DLMIMWCK01
---------------------	---	------------	----------------	---

Beschreibung des Kurses

Das Projekt dient zur Erstellung eines Aktionsplans zur digitalen Untersuchung und Vorfallbehandlung für ein gegebenes Bedrohungsszenario. Beginnend mit dem konkreten Verdacht auf eine computerkriminelle Handlung (z. B. eines vermuteten Server-Angriffs, dem Verlust von Kundendaten oder der Manipulation von Geschäftsdaten) planen die Studierenden die Durchführung einer digitalen Untersuchung für die elektronische Beweisführung und zur Sicherstellung gerichtsverwertbarer Beweise. Mit den gewonnenen Daten werden Risiken für betroffene Unternehmensprozesse evaluiert und Empfehlungen zur Vorfall-Behandlung und -Prävention gegeben.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende Methoden und Techniken der Computerforensik und deren Limitationen zu benennen.
- die von einer computerkriminellen Handlung betroffenen Systeme und Geschäftsprozesse zu identifizieren und eine Risikoabschätzung vorzunehmen.
- Maßnahmen zur Sicherstellung elektronischer Beweise zu empfehlen und deren Gerichtsverwertbarkeit zu evaluieren.
- Empfehlungen zur Vorfall-Kommunikation, -Reaktion und -Prävention zu entwickeln.

Kursinhalt

- Beginnend mit dem konkreten Verdacht auf eine computerkriminelle Handlung* erarbeiten die Studierenden einen Vorgehensplan, der folgende Maßnahmen abdeckt:
- Lokalisierung der betroffenen Systeme (Hardware und Software)
- Identifizierung der betroffenen Unternehmensprozesse
- Risikoabschätzung für die Auswirkung auf betroffene Unternehmensprozesse
- Kommunikation mit internen Abteilungen, Kooperationspartnern, Kunden und der Öffentlichkeit
- Identifizierung und Erhaltung relevanter Daten
- Examinierung der Daten
- Sicherstellung elektronischer Beweise und deren Gerichtsverwertbarkeit
- Empfehlungen zur Prävention

- *Beispiele für Verdachtsfälle sind ein vermuteter Server-Angriff, der Verlust von Kundendaten, die Manipulation von Geschäftsdaten, die Veröffentlichung interner Firmendaten, der Verdacht auf Produktpiraterie, die Inkonsistenz elektronischer Signaturen in Unternehmensdokumenten, die digitale Erpressung eines Entscheidungsträgers oder der Verdacht auf Industriespionage.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Aebi, D. (2013): Praxishandbuch Sicherer IT-Betrieb. Risiken erkennen, Schwachstellen beseitigen, IT-Infrastrukturen schützen. Springer, Berlin.
- Banaschik, M. (2011): Internationale E-Discovery und Information Governance. Praxislösungen für Juristen, Unternehmer und IT-Manager. Erich Schmidt Verlag, Berlin.
- Geschonneck, A. (2014): Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. dpunkt.verlag, Heidelberg.
- Hamid, J./Gianluigi, M./Lilburn, W. D. (2010): Handbook of electronic security and digital forensics. World Scientific Publishing, Singapur.
- Labudde, D./Spranger, M. (Hrsg.) (2017): Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. Springer, Berlin.
- Meier, S. (2017): Digitale Forensik in Unternehmen (Doktorarbeit). Universität Regensburg, Regensburg.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Projekt
-----------------------------------	---------------------------

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	Online Tests: Nein
Prüfungsleistung	Portfolio

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

Lehrmethoden		
Tutorielle Betreuung <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Lernmaterial <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Prüfungsleitfaden

Blockchain and Quantum Computing

Module Code: DLMCSEBCQC

Module Type see curriculum	Admission Requirements None	Study Level MA	CP 10	Student Workload 300 h
--------------------------------------	---------------------------------------	--------------------------	-----------------	----------------------------------

Semester / Term see curriculum	Duration Minimaldauer: 1 Semester	Regularly offered in WiSe/SoSe	Language of Instruction and Examination English
--	--	--	---

Module Coordinator

Enno Nagel (Blockchain) / Sydney Otten (Quantum Computing)

Contributing Courses to Module

- Blockchain (DLMCSEBCQC01)
- Quantum Computing (DLMCSEBCQC02)

Module Exam Type

Module Exam

Split Exam

Blockchain

- Study Format "Distance Learning": Written Assessment: Written Assignment

Quantum Computing

- Study Format "myStudies": *Type of examination*
- Study Format "Distance Learning": Oral Assignment

Weight of Module

see curriculum

Module Contents**Blockchain**

- Basic concepts of blockchain and related technologies
- Applications of blockchain and DLT
- Security
- Development of blockchain and DLT applications
- Social and legal aspects

Quantum Computing

- Physics of quantum computing
- Quantum computing models
- Quantum algorithms
- Quantum computing with the IBM framework Qiskit
- Applications, potential for and challenges of quantum computing

Learning Outcomes**Blockchain**

On successful completion, students will be able to

- outline the functions provided by and the technology used in blockchains.
- explain important applications of block chains, in particular BitCoin.
- demonstrate the technical architecture of blockchain applications.
- appraise the benefits and challenges of suggested blockchain applications.
- discuss the social and legal aspects of blockchain technology.

Quantum Computing

On successful completion, students will be able to

- outline the basic concepts of quantum mechanics as they relate to quantum computing.
- describe the computation models used in quantum computing.
- demonstrate the role of quantum computing for cryptography and other application areas.
- compare the theoretical and practical potential of quantum computing to classical computing.
- apply the concepts of quantum computing to develop simple programs within the Qiskit framework.

Links to other Modules within the Study Program

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

Links to other Study Programs of the University

All Bachelor Programmes in the IT & Technology field.

Blockchain

Course Code: DLMCSEBCQC01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	None

Course Description

Started by the cryptocurrency BitCoin, blockchain and related topics such as distributed ledger technologies and smart contracts have become increasingly important over the last few years and are claimed to be a major disruptive technologies. As BitCoin shows, systems that today need a trustworthy central coordinating body may become genuinely distributed systems without the need for such a body in the future. While blockchain has the potential for completely new types of applications, these suggested applications do not always make use of the strengths of the technology; rather, they simply provide a different approach to solving problems that could be solved more easily and efficiently using standard technologies such as database systems. Furthermore, blockchain applications have led to new social challenges and legal questions, such as the legal status of “smart contracts”. Different infrastructures such as Ethereum and Hyperledger have been developed to form the basis for blockchain applications. The goal of this course is to provide an understanding of the technical, as well as social and legal, aspects of blockchain and related technologies.

Course Outcomes

On successful completion, students will be able to

- outline the functions provided by and the technology used in blockchains.
- explain important applications of block chains, in particular BitCoin.
- demonstrate the technical architecture of blockchain applications.
- appraise the benefits and challenges of suggested blockchain applications.
- discuss the social and legal aspects of blockchain technology.

Contents

1. Basic Concepts
 - 1.1 The Functional View: Distributed Ledger Technologies
 - 1.2 The Technical View: Blockchain
 - 1.3 History of Blockchain and DLT
 - 1.4 Consensus Mechanisms
2. BitCoin
 - 2.1 The BitCoin Payment System
 - 2.2 The Technology Behind BitCoin

- 2.3 Security of BitCoin
- 2.4 Scalability and Other Limitations of BitCoin
- 2.5 BitCoin Derivatives and Alternatives
- 3. Smart Contracts and Decentralized Apps
 - 3.1 Smart Contracts
 - 3.2 Decentralized Apps (DApps)
 - 3.3 Ethereum
 - 3.4 Hyperledger
 - 3.5 Alternative Platforms for Smart Contracts and DApps
- 4. Security of Block Chain and DLT
 - 4.1 Cryptology Used
 - 4.2 Attacks on Blockchain and DLT
 - 4.3 Resolving Bugs and Security Holes
 - 4.4 Long-Term Security
- 5. Block Chain and DLT Application Scenarios
 - 5.1 Benefits and Limits of Applying Blockchain and DLT
 - 5.2 Registers for Land and Other Property
 - 5.3 Applications in the Supply Chain
 - 5.4 Applications in Insurance
 - 5.5 Initial Coin Offerings for Sourcing Capital
 - 5.6 Examples of Further Applications
- 6. Development of Blockchain and DLT Applications
 - 6.1 Architecture of Blockchain and DLT Applications
 - 6.2 Platform Selection
 - 6.3 Design of Blockchain and DLT Applications
- 7. Blockchain and Society
 - 7.1 (Mis-)Trust in Institutions
 - 7.2 Blockchain and the Environment
 - 7.3 Cyber-Currencies in the Darknet
 - 7.4 ICO Fraud
- 8. Legal Aspects
 - 8.1 DLT and Smart Contracts as Legal Contracts
 - 8.2 Cryptocurrencies as Legal Currencies

8.3 Regulation of ICOs

8.4 Data Protection / Privacy in Blockchains

Literature

Compulsory Reading

Further Reading

- De Filippi, P., & Wright, A. (2018). Blockchain and the law. The rule of code. Cambridge, MA: Harvard University Press.
- Meinel, C., Gayvoronskaya, T. & Schnjakin, M. (2018). Blockchain. Hype or innovation. Potsdam: Universitätsverlag Potsdam.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system [white paper]. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- Tapscott, D., & Tapscott, N. (2018). Blockchain revolution. How the technology behind bitcoin is changing money, business, and the world. New York, NY: Portfolio/Penguin.
- Xu, W., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Cham: Springer.

Study Format Distance Learning

Study Format Distance Learning	Course Type Theory Course
--	-------------------------------------

Information about the examination	
Examination Admission Requirements	Online Tests: yes
Type of Exam	Written Assessment: Written Assignment

Student Workload					
Self Study 110 h	Contact Hours 0 h	Tutorial/Tutorial Support 20 h	Self Test 20 h	Independent Study 0 h	Hours Total 150 h

Instructional Methods		
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Learning Material <input checked="" type="checkbox"/> Course Book <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Slides	Exam Preparation <input checked="" type="checkbox"/> Online Tests <input checked="" type="checkbox"/> Guideline

Quantum Computing

Course Code: DLMCSEBCQC02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Quantum computing is a completely new paradigm for the architecture of computers. It currently is in the early stage of development but has the potential to speed up certain kinds of computations, not just by orders of magnitude but by moving them from exponential to linear growth. One of the issues that will be affected is the prime factorization of large numbers which currently forms the basis for important cryptographic algorithms, in particular the RSA algorithm which would in that case would no longer be secure. This course gives an introduction to the physics behind quantum computing and the computation models used. Students are familiarized with the most important algorithms for quantum computing and write a few programs for quantum computers. The application potential and challenges of quantum computing are also discussed.

Course Outcomes

On successful completion, students will be able to

- outline the basic concepts of quantum mechanics as they relate to quantum computing.
- describe the computation models used in quantum computing.
- demonstrate the role of quantum computing for cryptography and other application areas.
- compare the theoretical and practical potential of quantum computing to classical computing.
- apply the concepts of quantum computing to develop simple programs within the Qiskit framework.

Contents

1. Basic concepts
 - 1.1 Quantum physics as a basis for computing
 - 1.2 Types of quantum computers
 - 1.3 Qbits
 - 1.4 Linear algebra
2. The physics of quantum computers
 - 2.1 Basic concepts of quantum mechanics
 - 2.2 Spin and entanglement
 - 2.3 Architecture of quantum computers

- 2.4 Noise and error correction
- 2.5 Current state and outlook
3. Quantum computing models
 - 3.1 Quantum gates and circuits
 - 3.2 Single qubit quantum systems
 - 3.3 Multiple qubit quantum systems
4. Quantum algorithms
 - 4.1 Computability and complexity in quantum computing
 - 4.2 Quantum Fourier transform
 - 4.3 The Shor algorithm
 - 4.4 The Grover algorithm
5. Quantum computing with the IBM framework Qiskit
 - 5.1 Overview of Qiskit and the IBM Q Provider
 - 5.2 Quantum circuits in Qiskit
 - 5.3 First steps in programming with Qiskit
6. Applications, potential and challenges of quantum computing
 - 6.1 Applications of quantum computing
 - 6.2 Quantum cryptography and post-quantum cryptography
 - 6.3 Quantum supremacy

Literature

Compulsory Reading

Further Reading

- Mermin, N. D. (2007). Quantum computer science: An introduction. Cambridge University Press.
- Nielsen, M. A., & Chuang, I. L. (2000). Quantum computation and quantum information. Cambridge University Press.
- Rieffel, E. G., & Polak, W. H. (2011). Quantum computing: A gentle introduction. MIT Press.

Study Format myStudies

Study Format myStudies	Course Type Theory Course
----------------------------------	-------------------------------------

Information about the examination	
Examination Admission Requirements	Online Tests: no
Type of Exam	

Student Workload					
Self Study 110 h	Contact Hours 0 h	Tutorial/Tutorial Support 20 h	Self Test 20 h	Independent Study 0 h	Hours Total 150 h

Instructional Methods
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions

Study Format Distance Learning

Study Format Distance Learning	Course Type Theory Course
--	-------------------------------------

Information about the examination	
Examination Admission Requirements	Online Tests: yes
Type of Exam	Oral Assignment

Student Workload					
Self Study 110 h	Contact Hours 0 h	Tutorial/Tutorial Support 20 h	Self Test 20 h	Independent Study 0 h	Hours Total 150 h

Instructional Methods		
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Learning Material <input checked="" type="checkbox"/> Course Book <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Slides	Exam Preparation <input checked="" type="checkbox"/> Online Tests <input checked="" type="checkbox"/> Guideline

Sichere Software-Entwicklung

Modulcode: DLMCSEEDSO_D

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

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

Modulverantwortliche(r)

Prof. Dr. Petra Beenken (Sichere Software-Entwicklung) / Dilan Özdemir-Kaluk (Projekt: Sichere Software-Implementierung)

Kurse im Modul

- Sichere Software-Entwicklung (DLMCSEEDSO01_D)
- Projekt: Sichere Software-Implementierung (DLMCSEEDSO02_D)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Sichere Software-Entwicklung

- Studienformat "Fernstudium": Klausur,

Projekt: Sichere Software-Implementierung

- Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls**Sichere Software-Entwicklung**

- Sicheres Software Design und -Implementierung
- Sicherheitsprüfung und -Auditierung
- Patch- und Schwachstellenmanagement
- Software-Lebenszyklus

Projekt: Sichere Software-Implementierung

- Sicheres Software Design und -Implementierung
- Sicherheitsprüfung und -Auditierung
- Patch- und Schwachstellenmanagement
- Software-Lebenszyklus

Qualifikationsziele des Moduls**Sichere Software-Entwicklung**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sichere Anwendungen zu entwerfen.
- zu verstehen, was zu Software-Kompromittierung führt.
- gewöhnliche Kodierungsfehler zu vermeiden.
- den sicheren Software-Lebenszyklus zu steuern.
- ein strenges Sicherheitsprüfungssystem anzuwenden.
- die Offenlegung von Schwachstellen zu steuern.

Projekt: Sichere Software-Implementierung

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Sicherheitsmaßnahmen für ein einfaches Software-Projekt zu entwerfen.
- häufige Kodierungs- und Designfehler zu vermeiden.
- zu definieren, welche Schritte erforderlich sind, um sicheren Code zu implementieren.
- einen Prozess zu schaffen, der die kontinuierliche Sicherheit der Anwendung während ihrer gesamten Lebensdauer gewährleistet.
- die Offenlegung von Schwachstellen effektiv zu nutzen.

Bezüge zu anderen Modulen im Studiengang

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

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik

Sichere Software-Entwicklung

Kurscode: DLMCSEEDSO01_D

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

Beschreibung des Kurses

Der Angriff auf Schwachstellen in unsicherer Software ist ein führender Angriffsweg für Kriminelle und böswillige staatliche Akteure. Das Auffinden unbekannter so genannter Zero-Day-Schwachstellen ist ein zentrales Werkzeug für professionelle Kriminelle. Daher ist es von größter Bedeutung, sichere Software zu entwickeln und zu implementieren. Zuerst müssen wir allgemeine Softwareschwächen verstehen und diese dann so früh wie möglich in der Entwicklung und im Software-Lebenszyklus durch eine "Security-by-Design"-Philosophie vermeiden. Außerdem soll ein Prozess für Sicherheitstests und die Offenlegung von Schwachstellen durchgeführt und gesteuert werden. Die Entwicklung und Implementierung von zeitgerechten Softwareupdates „Patches“ ist essentiell.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sichere Anwendungen zu entwerfen.
- zu verstehen, was zu Software-Kompromittierung führt.
- gewöhnliche Kodierungsfehler zu vermeiden.
- den sicheren Software-Lebenszyklus zu steuern.
- ein strenges Sicherheitsprüfungssystem anzuwenden.
- die Offenlegung von Schwachstellen zu steuern.

Kursinhalt

1. Security by Design
 - 1.1 IT-Support und Test mit der „Shift Left“-Methodik
 - 1.2 Infrastructure as a Code
 - 1.3 Vorteile einer frühzeitigen Berücksichtigung der IT-Sicherheit
2. Privacy by Design
 - 2.1 Verschlüsselung
 - 2.2 Differentielle Privatheit (Differential Privacy)
 - 2.3 Zero-Knowledge-Beweise und Protokolle
3. Tests und Audits
 - 3.1 Unit-Tests

- 3.2 Sicherheitstests
- 3.3 Sicherheitsauditierung von Quelltext
4. 4. Sicherheit der Software-Lieferkette
 - 4.1 Paketsicherheit
 - 4.2 Containersicherheit
 - 4.3 Auswahl einer Programmiersprache
5. Gängige Programmierfehler
 - 5.1 Klassen von Bugs
 - 5.2 Quellen von Bugs
 - 5.3 Schweregrad der Bugs
6. Projektmanagement
 - 6.1 Der Software-Lebenszyklus
 - 6.2 Schwachstellen-Management
 - 6.3 Patch-Management
 - 6.4 Management von Pentests- und Bug-Bounty-Programmen
7. DevSecOps
 - 7.1 DevOps
 - 7.2 Cloud-Sicherheit
 - 7.3 Continuous Integration, Continuous Delivery and Deployment (CI/CD)
 - 7.4 Ephemere Prozesse
 - 7.5 Automatisierung

Literatur

Pflichtliteratur

Weiterführende Literatur

- Adkins, H. et al (2020): Building Secure and Reliable Systems. O'Reilly Media, Newton, MA.
- Common Weakness Enumeration, <https://cwe.mitre.org/>
- Dwork, C. / Roth, A. (2014): The Algorithmic Foundations of Differential Privacy. In Foundations and Trends in Theoretical Computer Science Vol. 9, Nos. 3–4 (2014) 211–407.
- The Open Web Application Security Project, <https://owasp.org/>

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

Projekt: Sichere Software-Implementierung

Kurscode: DLMCSEEDSO02_D

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 5	Zugangsvoraussetzungen DLMCSEEDSO01_D oder DLMCSEEDSO01_E
---------------------	---	------------	----------------	--

Beschreibung des Kurses

Frei nach dem Spruch „Software is eating the world“ kann es sich keine Organisation leisten, unsicheren Code einzusetzen, ohne letztendlich schlimme Folgen zu erleiden. In diesem Projekt sollen Studierende eine sichere Anwendungsimplementierung in Angriff nehmen und einen Bericht schreiben, in dem die getroffenen Entscheidungen zur Gewährleistung der Sicherheit des laufenden Systems begründet werden.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Sicherheitsmaßnahmen für ein einfaches Software-Projekt zu entwerfen.
- häufige Kodierungs- und Designfehler zu vermeiden.
- zu definieren, welche Schritte erforderlich sind, um sicheren Code zu implementieren.
- einen Prozess zu schaffen, der die kontinuierliche Sicherheit der Anwendung während ihrer gesamten Lebensdauer gewährleistet.
- die Offenlegung von Schwachstellen effektiv zu nutzen.

Kursinhalt

- Für ein gegebenes Problem und/oder einen gegebenen Kontext entwirft und entwickelt der Studierende ein einfaches Softwareprojekt und reicht dann einen Bericht, Code und Daten ein, die die Entscheidungen des Sicherheitsdesigns sowie Pläne für den zukünftigen Software-Lebenszyklus beschreiben. Spezifische Projekte werden vom Tutor zur Verfügung gestellt, aber Vorschläge der Studierenden können berücksichtigt werden.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Adkins, H. et al (2020): Building Secure and Reliable Systems. 1st edition, O'Reilly Media, Newton, MA.
- Common Weakness Enumeration, <https://cwe.mitre.org/>
- Dwork, C. / Roth, A. (2014): The Algorithmic Foundations of Differential Privacy. In Foundations and Trends in Theoretical Computer Science Vol. 9, Nos. 3–4 (2014) 211–407.
- The Open Web Application Security Project, <https://owasp.org/>

Studienformat Fernstudium

Studienform Fernstudium	Kursart Projekt
-----------------------------------	---------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Lernmaterial <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Prüfungsleitfaden

Transformation von Organisationen

Modulcode: DLMCSDWTO_D

Modultyp s. Curriculum	Zugangsvoraussetzungen keine	Niveau MA	CP 10	Zeitaufwand Studierende 300 h
----------------------------------	--	---------------------	-----------------	---

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

Modulverantwortliche(r)

Marc Rosca (Instrumente der Organisationsanalyse) / Prof. Dr. André Köhler (Management von IT-Services und IT-Architekturen)

Kurse im Modul

- Instrumente der Organisationsanalyse (DLMWPWOAE01)
- Management von IT-Services und IT-Architekturen (MWIT02)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Instrumente der Organisationsanalyse

- Studienformat "Fernstudium": Klausur, 90 Minuten

Management von IT-Services und IT-Architekturen

- Studienformat "Fernstudium": Klausur, 90 Minuten

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls**Instrumente der Organisationsanalyse**

- Organisation
- Organisationsforschung
- Organisationsdiagnostik
- Organisationsanalyse
- Praktische Anwendung in spezifischen Bereichen

Management von IT-Services und IT-Architekturen

- Grundlagen IT-Service Management und Begriffsbildung
- IT Infrastructure Library (ITIL)
- IT-Outsourcing
- IT-Architekturmanagement
- IT-Anwendungsportfolio-Management
- Aufbauorganisation der IT- und Architektur-Governance

Qualifikationsziele des Moduls**Instrumente der Organisationsanalyse**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sich differenziert mit dem Organisationsbegriff auseinanderzusetzen.
- die Möglichkeiten der Organisationsdiagnostik zu beurteilen.
- ausgewählte Instrumente der Organisations- und Teamdiagnose einzusetzen.
- Organisationsdiagnostische Maßnahmen durchzuführen, auszuwerten und reflektieren zu können.
- spezifische organisationale Analysen zu bearbeiten.

Management von IT-Services und IT-Architekturen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundprinzipien von IT-Strategie, IT-Governance und IT-Architekturmanagement zu benennen, zu erläutern und voneinander abzugrenzen .
- die typischen Aktivitäten des IT-Architekturmanagements, deren Zusammenhänge und deren Abhängigkeiten zu erläutern und voneinander abzugrenzen.
- die Grundlagen und Herausforderungen des IT-Service Managements zu erläutern.
- die Motivation und den Aufbau der IT Infrastructure Library (ITIL) zu beschreiben, die Hauptelemente zu erläutern und konkrete Aktivitäten im Service Lifecycle zu verorten.
- die Aktivitäten der ITIL-Governance und ITIL-Operational-Prozesse zu beschreiben und voneinander abzugrenzen.

Bezüge zu anderen Modulen im Studiengang

Baut auf Modulen im Bereich Betriebswirtschaft & Management und Informatik & Software-Entwicklung auf.

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich Wirtschaft & Management und IT & Technik.

Instrumente der Organisationsanalyse

Kurscode: DLMWPWOAE01

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

Beschreibung des Kurses

Organisationen sind mehr denn je lebendige Organismen, die sich aufgrund der äußeren Veränderungen auch im Inneren verändern und neuen Rahmenbedingungen anpassen müssen. Der Kurs setzt sich mit einer differenzierten Betrachtung von unternehmerisch ausgerichteten Organisationen, deren Zielen, möglicher Strategien, ihrer Funktion und Leistungsvermögen auseinander. Er beleuchtet die Möglichkeiten der Organisationsforschung und deren Forschungsfelder, um anschließend auf die Ziele, Möglichkeiten und Anwendungsfelder der Diagnose von Organisationen einzugehen. Es werden verschiedene Methoden und Instrumente der Organisationsdiagnose vorgestellt mit dem Ziel diese im organisationalen Analyseprozess einzusetzen. Damit wird es den Studierenden möglich, Veränderungsmaßnahmen auf der Basis diagnostischer Instrumente einzuleiten und durchzuführen bzw. solche Maßnahmen zu beurteilen. Dabei geht der Kurs auch auf die praktische Anwendung der im betrieblichen Alltag auftretenden Themenfelder wie der Analyse von Change Managementprozessen, von Karrieren und in Verbindung mit der Risikoprüfung beim Kauf von Unternehmen bzw. Unternehmensbeteiligungen (Due Dilligence) ein. Den Studierenden wird so das Spektrum und die Einsatzmöglichkeiten der Maßnahmen und Methoden einer gezielten Organisationsanalyse durch diagnostische Maßnahmen vermittelt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sich differenziert mit dem Organisationsbegriff auseinanderzusetzen.
- die Möglichkeiten der Organisationsdiagnostik zu beurteilen.
- ausgewählte Instrumente der Organisations- und Teamdiagnose einzusetzen.
- Organisationsdiagnostische Maßnahmen durchzuführen, auszuwerten und reflektieren zu können.
- spezifische organisationale Analysen zu bearbeiten.

Kursinhalt

1. Organisation
 - 1.1 Der Organisationsbegriff
 - 1.2 Ziele und Strategien einer Organisation
 - 1.3 Funktion und Leistung von Organisationen
 - 1.4 Rolle von Menschen in Organisationen

- 1.5 Unterschiede zwischen Organisationen
2. Organisationsforschung
 - 2.1 Perspektiven der Organisationsforschung
 - 2.2 Forschungsfelder
 - 2.3 Empirie der Organisationsforschung
3. Organisationsdiagnostik
 - 3.1 Definition und Ziele der Organisationsdiagnostik
 - 3.2 Anwendungsfelder der Organisationsdiagnostik
 - 3.3 Die Organisationsdiagnose als Managementinstrument
 - 3.4 Zielgruppen organisationsdiagnostischer Erkenntnisse
 - 3.5 Ausgewählte Instrumente der Team- und Organisationsdiagnose
4. Organisationsanalyse
 - 4.1 Die Organisationsanalyse
 - 4.2 Vorüberlegungen und Analyseprozess
 - 4.3 Konzeption und Operationalisierung
 - 4.4 Erhebungsmethoden
 - 4.5 Erhebung und Auswertung
 - 4.6 Präsentation der Analyse und Reflexion
5. Praktische Anwendung in spezifischen Bereichen
 - 5.1 Analyse von Veränderungsprozessen
 - 5.2 Netzwerkanalyse
 - 5.3 Analyse von Karrieren in Organisationen
 - 5.4 Organisationsanalyse und Due Diligence

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

- Blickle, G./ Schaper, N./ Nerdinger, F. W. (2014): Springer-Lehrbuch. Arbeits- und Organisationspsychologie. Springer, Berlin.
- Bornewasser, M. (2009): Organisationsdiagnostik und Organisationsentwicklung. Kohlhammer, Stuttgart.
- Doppler, K./Lauterburg, C. (2014): Change Management. Den Unternehmenswandel gestalten. 13. Auflage, Campus Verlag, Frankfurt/New York.
- Elbe, M. (2015): Organisationsdiagnose – Methoden – Fallstudien – Reflexionen. Schneider Verlag, Hohengehren.
- Felfe, J./Liepmann, D. (2007): Organisationsdiagnostik. Hogrefe Verlag, Göttingen.
- Pelzmann, S./Strümpf, B. (2012): Integrative Tools für die Team- und Organisationsdiagnose. Wirksam beraten. Springer VS, Wiesbaden.
- Pelzmann, S./Strümpf, B. (2018): Integrative Tools für die Team- und Organisationsdiagnose. Wirksam beraten. 2. Auflage, Springer, Berlin.
- Schuler, H./Moser, K. (2014): Lehrbuch Organisationspsychologie. 5. Auflage, Hogrefe (vorm. Verlag Hans Huber), Göttingen.
- Titscher, S./Meyer, M./ Mayrhofer, W. (2008): Organisationsanalyse Konzepte und Methoden. UTB, Wien.
- Titscher, S./ Meyer, M./ Mayrhofer, W. (2010): Praxis der Organisationsanalyse. Anwendungsfelder und Methoden. UTB, Wien.
- Werner, C./Elbe, M. (2014): Handbuch Organisationsdiagnose (Schriftenreihe des internationalen Hochschulverbunds IUNworld). Herbert Utz Verlag, München.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

Management von IT-Services und IT-Architekturen

Kurscode: MWIT02

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 5	Zugangsvoraussetzungen 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. 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. Die Aufgabe des IT-Architekturmanagements 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 benennen, zu erläutern und voneinander abzugrenzen .
- die typischen Aktivitäten des IT-Architekturmanagements, deren Zusammenhänge und deren Abhängigkeiten zu erläutern und voneinander abzugrenzen.
- die Grundlagen und Herausforderungen des IT-Service Managements zu erläutern.
- die Motivation und den Aufbau der IT Infrastructure Library (ITIL) zu beschreiben, die Hauptelemente zu erläutern und konkrete Aktivitäten im Service Lifecycle zu verorten.
- die Aktivitäten der ITIL-Governance und ITIL-Operational-Prozesse zu beschreiben und voneinander abzugrenzen.

Kursinhalt

1. Grundlagen und Begriffe zum IT-Servicemanagement
 - 1.1 IT-Dienstleistungen (auch: IT-Services, engl.: IT services)
 - 1.2 IT-Servicemanagement
2. IT Infrastructure Library (ITIL)
 - 2.1 Service Lifecycle und Prozessgruppen in ITIL
 - 2.2 Service Strategy
 - 2.3 Continual Service Improvement

3. ITIL – Service Design
 - 3.1 Service Level Management
 - 3.2 Service Catalog Management
 - 3.3 Availability Management
 - 3.4 Weitere Prozesse im Service Design
4. ITIL – Service Transition
 - 4.1 Transition Planning and Support
 - 4.2 Change Management
 - 4.3 Service Asset and Configuration Management (SACM)
 - 4.4 Weitere Prozesse in der Service Transition
5. ITIL – Service Operation
 - 5.1 Event Management
 - 5.2 Incident Management
 - 5.3 Problem Management
 - 5.4 Weitere Prozesse in der Service Operation
6. Grundlagen und Begriffe zum IT-Architekturmanagement
 - 6.1 IT-Unternehmensarchitektur
 - 6.2 Ziele von Enterprise Architecture Management
 - 6.3 Prozesse im Management von IT-Unternehmensarchitekturen
7. IT-Anwendungsportfoliomanagement
 - 7.1 Überblick über das IT-Anwendungsportfoliomanagement
 - 7.2 Anwendungshandbuch
 - 7.3 Portfolioanalyse
 - 7.4 Bebauungsplanung
8. Architektur-Governance
 - 8.1 Aufbauorganisation
 - 8.2 Entwicklung und Durchsetzung von Richtlinien
 - 8.3 Projektbegleitung

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

- Beims, M. (2014): IT-Service Management in der Praxis mit ITIL. 4. Auflage, Carl Hanser, München.
- Böttcher, R. (2013): IT-Service Management mit ITIL – 2011 Edition. Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen. Heise, dpunkt, Heidelberg.
- Keller, W. (2012): IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung. 2. Auflage, dpunkt, Heidelberg.
- Kleiner, F. (2013): IT Service Management. Aus der Praxis für die Praxis. Springer Vieweg, Heidelberg.
- Scholderer, R. (2016): Management von Service-Level-Agreements. Methodische Grundlagen und Praxislösungen mit COBIT, ISO 20000 und ITIL. 2. Auflage, dpunkt, Heidelberg.
- Ward, J./Peppard, J. (2002): Strategic Planning for Information Systems. 3. Auflage, Wiley, Hoboken, NJ.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

IT-Recht in der IT-Sicherheit

Modulcode: DLMCSEEITLS_D

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

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

Modulverantwortliche(r)

Prof. Dr. Sascha Stiegler (Nationales und internationales IT-Recht) / Prof. Dr. Sascha Stiegler (Seminar: Rechtliche Rahmenbedingungen der IT-Sicherheit)

Kurse im Modul

- Nationales und internationales IT-Recht (DLMIMWITR01)
- Seminar: Rechtliche Rahmenbedingungen der IT-Sicherheit (DLMCSEEITLS01_D)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Nationales und internationales IT-Recht

- Studienformat "Fernstudium": Klausur, 90 Minuten

Seminar: Rechtliche Rahmenbedingungen der IT-Sicherheit

- Studienformat "Fernstudium": Schriftliche Ausarbeitung; Seminararbeit

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls**Nationales und internationales IT-Recht**

- Abgrenzung des IT-Rechts
- Grundlegende Rechtsauffassungen
- Relevante Rechtsbereiche
- Europäisches IT-Recht
- Transnationales IT-Recht

Seminar: Rechtliche Rahmenbedingungen der IT-Sicherheit

Die Einhaltung der Gesetze ist ein wichtiger Faktor für die Sicherheit in Organisationen. Die Studierenden müssen die verschiedenen rechtlichen Rahmenbedingungen und Rechtsprechungen verstehen, die für ihre Arbeit gelten können. Geltendes Recht spielt auch eine Rolle bei der Verfolgung von Kriminellen, die eine Organisation angreifen. Die Unterstützung zur Beweissicherung spielt dabei eine Schlüsselrolle. In diesem Modul untersuchen wir diese rechtlichen Rahmenbedingungen und wenden sie auf realistische Probleme aus dem Bereich der Computersicherheit an.

Qualifikationsziele des Moduls

Nationales und internationales IT-Recht

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Unterschiede nationaler, transnationaler und internationaler Rechtssysteme zu benennen und zu erläutern.
- Schnittstellen zwischen allgemeinen Rechtsauffassungen und IT-relevantem Recht zu identifizieren.
- Rechtliche Voraussetzungen zur IT-Vertragsgestaltung zu benennen und deren Auswirkung auf die (elektronische) Kommerzialisierung von IT-Produkten oder -Dienstleistungen zu bewerten.
- Die Auswirkung der Europäischen Datenschutzgrundverordnung auf Geschäftsprozesse zu beurteilen und Empfehlungen zur Implementierung zu geben.
- Rechtsauffassungen ausgewählter transnationaler Institutionen zu benennen und deren Auswirkungen auf die internationale IT-Rechtsprechung einzuschätzen.

Seminar: Rechtliche Rahmenbedingungen der IT-Sicherheit

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- zu verstehen, wie Gesetze im Cyberraum und auf IT-Sicherheits-Organisationen und Unternehmen angewendet werden.
- die rechtlichen Grenzen der Verfolgung von Kriminellen für die Strafverfolgungsbehörden und die Bedeutung der Beweissicherung zu verstehen.
- die Unterschiede im internationalen Recht bei der Anwendung von Computeroperationen anzuerkennen.
- zu verstehen, wie rechtliche Rahmenbedingungen die Einhaltung von Computersicherheitsvorschriften fördern.

Bezüge zu anderen Modulen im Studiengang

Baut auf Modulen aus dem Bereich Recht auf

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich
Wirtschaft & Management

Nationales und internationales IT-Recht

Kurscode: DLMIMWITR01

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

Beschreibung des Kurses

Der Kurs stellt vertiefend nationale und internationale rechtliche Rahmenbedingungen der Informationsverarbeitung für Unternehmen vor. Nach einer Betrachtung der Unterschiede internationaler Rechtssysteme erfolgt eine Einführung in solche rechtlichen Konstrukte, die als Basis für die Entwicklung der IT-relevanten Gesetzgebung dienen. In der Folge werden Rechtsbereiche aus der Sicht konkreter anwendungsorientierter Geschäftsszenarien, wie Vertragsrecht, Lizenzierung und Patentierung, behandelt. Einer Einführung in das EU-Rechtssystem folgt eine ausführliche Auseinandersetzung mit der Europäischen Datenschutz-Grundverordnung, die als wichtigstes Rahmenwerk des IT-Rechts in Europa zunehmend an internationaler Bedeutung gewinnt. Dies leitet in eine Betrachtung transnationaler Rechtssysteme über und schließt mit Empfehlungen überstaatlicher Organisationen ab.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Unterschiede nationaler, transnationaler und internationaler Rechtssysteme zu benennen und zu erläutern.
- Schnittstellen zwischen allgemeinen Rechtsauffassungen und IT-relevantem Recht zu identifizieren.
- Rechtliche Voraussetzungen zur IT-Vertragsgestaltung zu benennen und deren Auswirkung auf die (elektronische) Kommerzialisierung von IT-Produkten oder -Dienstleistungen zu bewerten.
- Die Auswirkung der Europäischen Datenschutzgrundverordnung auf Geschäftsprozesse zu beurteilen und Empfehlungen zur Implementierung zu geben.
- Rechtsauffassungen ausgewählter transnationaler Institutionen zu benennen und deren Auswirkungen auf die internationale IT-Rechtsprechung einzuschätzen.

Kursinhalt

1. Einführung
 - 1.1 Fallbasiertes (Common Law) vs. kodifiziertes Recht (Civil Law)
 - 1.2 Internationales, Transnationales und Europäisches Recht
 - 1.3 Abgrenzung des IT-Rechts von anderen Rechtsgebieten
2. Grundlegende Rechtsauffassungen

- 2.1 Geistiges Eigentum und Urheberrecht
 - 2.2 Informations- und Nachweispflichten nach bürgerlichem Recht
 - 2.3 Grundlagen des Telemedienrechts
 - 2.4 Grundlagen des Telekommunikationsrechts
 - 2.5 Rechtsauffassungen zu Datenschutz und Informationssicherheit
3. Relevante Rechtsbereiche
 - 3.1 Allgemeine Geschäftsbedingungen
 - 3.2 Vertragsrecht der IT und Vertragsgestaltung
 - 3.3 IT-Dienstleistungsverträge
 - 3.4 Softwareverträge, Lizenzmodelle und General Public License
 - 3.5 Elektronischer Geschäftsverkehr (E-Commerce)
 - 3.6 Signaturrecht
 - 3.7 Patentierung von Software
4. Europäisches IT-Recht
 - 4.1 EU-Regulierungen, -Direktiven, -Entscheidungen, und -Empfehlungen
 - 4.2 Verhältnis zur nationalen Rechtsordnung
 - 4.3 EU-Regularien mit Bezug zum IT-Recht
 - 4.4 Europäische Datenschutz-Grundverordnung (DSGVO)
 - 4.5 Implementierungsansätze der DSGVO
 - 4.6 Die DSGVO als Basis internationaler Rechtsprechung
5. Transnationales IT-Recht
 - 5.1 Internet-Recht
 - 5.2 Domainrecht
 - 5.3 Rechtliche Betrachtung sozialer Medien
 - 5.4 WTO Information Technology Agreement
 - 5.5 OECD-Richtlinien und Empfehlungen
 - 5.6 Empfehlungen der United Nations Information and Communication Technologies Task Force

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

- Auer-Reinsdorff, Astrid/Conrad, Isabell, Handbuch IT- und Datenschutzrecht, 3. Auflage, München 2019.
- Hetmank, Sven, Internetrecht, Wiesbaden 2016.
- Leupold, Andreas/Wiebe, Andreas/Glossner, Silke, IT-Recht, 4. Auflage, München 2021.
- Redeker, Helmut, IT-Recht, 8. Auflage, München 2023.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Musterklausur <input checked="" type="checkbox"/> Online Tests

Seminar: Rechtliche Rahmenbedingungen der IT-Sicherheit

Kurscode: DLMCSEEITLS01_D

Niveau	Kurs- und Prüfungssprache	SWS	CP	Zugangsvoraussetzungen
MA	Deutsch		5	DLMIGCR01-01 oder DLMIGCR01-01_E; DLMIMWITR01 oder DLMIMWITR01_E

Beschreibung des Kurses

Computersicherheit funktioniert nicht in einem rechtlichen Vakuum. Sie unterliegt einem Rahmenwerk in Bezug auf die Anwendbarkeit internationale Rechtes im Cyberraum, nationale Cybersicherheitsstrategien, und nationalen Grundsätzen und Gesetzgebung. Durch die globale Natur des Cyberraumes müssen Organisationen oft unter unterschiedlichen Gerichtsbarkeiten mit einer Vielzahl von Gesetzen arbeiten. Kriminelle nutzen dies aus, indem sie ihrer wichtigsten Operationen außerhalb der Reichweite der Strafverfolgung ihres Opfers stellen. Staatliche Akteure und nicht staatliche Akteure operieren in rechtlichen Grauzonen, um ihre Ziele zu verfolgen. Dazu erarbeiten internationale Organisationen wie z.B. die EU, OSZE und ASEAN Konformitätsrahmen und Mechanismen. In diesem Seminar untersuchen wir Fälle und rechtliche Rahmenbedingungen, welche IT-Sicherheitspersonal berücksichtigen muss.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- zu verstehen, wie Gesetze im Cyberraum und auf IT-Sicherheits-Organisationen und Unternehmen angewendet werden.
- die rechtlichen Grenzen der Verfolgung von Kriminellen für die Strafverfolgungsbehörden und die Bedeutung der Beweissicherung zu verstehen.
- die Unterschiede im internationalen Recht bei der Anwendung von Computeroperationen anzuerkennen.
- zu verstehen, wie rechtliche Rahmenbedingungen die Einhaltung von Computersicherheitsvorschriften fördern.

Kursinhalt

- Studierende erhalten einen Aspekt des Rechts oder einen Rechtsfall, den sie bearbeiten und über den sie berichten sollen. Von besonderer Bedeutung ist es, zu verstehen, welche möglichen Folgen der Fall oder das Gesetz für eine Organisation und Unternehmen haben wird. Spezifische Rechtstexte oder Rechtsfälle werden vom Tutor zur Verfügung gestellt, aber Vorschläge der Studierenden können berücksichtigt werden.

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

- Clarke, R. A. / Knake R. K. (2010): Cyber War. 1st edition, HarperCollins, New York City, NY.
- Lusthaus, J. (2018): Industry of Anonymity. Harvard University Press, Cambridge, MA.
- Schmitt, M. N. (ed.) (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge.
- Schneier, B. (2015): Data and Goliath. 1st edition, W. W. Norton & Company, New York City, NY.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Seminar
-----------------------------------	---------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Lernmaterial <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Prüfungsleitfaden

Audit- and Security Testing

Module Code: DLMCSEEST_E

Module Type see curriculum	Admission Requirements	Study Level MA	CP 10	Student Workload 300 h
--------------------------------------	-------------------------------	--------------------------	-----------------	----------------------------------

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

Module Coordinator

Dr. Christian Prause (Attack Models and Auditing) / Dr. Radiah Rivu (Seminar: IT Security Tests)

Contributing Courses to Module

- Attack Models and Auditing (DLMCSEEST01_E)
- Seminar: IT Security Tests (DLMCSEEST02_E)

Module Exam Type

Module Exam

Split Exam

Attack Models and Auditing

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

Seminar: IT Security Tests

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

Weight of Module

see curriculum

Module Contents**Attack Models and Auditing**

- Threat modelling
- Software testing and verification
- Pentesting tools
- Self-assessment and third-party audits
- Ethical hacking

Seminar: IT Security Tests

Software and system auditing; Pentesting; Red/Blue teams; Bug Bounty programs

Learning Outcomes**Attack Models and Auditing**

On successful completion, students will be able to

- plan what to test and audit for.
- understand common pentesting tools.
- understand software testing and verification.
- organize self-assessments of the implemented ISMS.
- familiarize with widely used cybersecurity audit frameworks.
- run remote system audits.

Seminar: IT Security Tests

On successful completion, students will be able to

- understand how bug bounty programs work.
- understand how to run a red/blue team or pentesting exercise.
- write a report showing aptitude in the subject.

Links to other Modules within the Study Program

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

Links to other Study Programs of the University

All Master Programs in the IT & Technology fields

Attack Models and Auditing

Course Code: DLMCSEEST01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The cybersecurity lifecycle comprehends a range of activities, where “checking” the implemented security concept provides a feedback loop to continuously improve the designed security levels. In practice, cybersecurity checks include an initial threat modeling step before the right tools and techniques can be used to test the security of the software or system. This can be a type of ethical hacking (e.g., pentesting, red/blue team exercise or bug bounty program), or a self-assessment or this-party audit of the deployed information security management system (ISMS).

Course Outcomes

On successful completion, students will be able to

- plan what to test and audit for.
- understand common pentesting tools.
- understand software testing and verification.
- organize self-assessments of the implemented ISMS.
- familiarize with widely used cybersecurity audit frameworks.
- run remote system audits.

Contents

1. Threat Modelling
 - 1.1 System Security Life Cycle
 - 1.2 Modelling applications and profiling threats
 - 1.3 Security testing based on a threat model
 - 1.4 OWASP Threat Dragon and Microsoft Threat Modelling Tool
2. Ethical Hacking
 - 2.1 Legal and compliance framework
 - 2.2 Pentesting process
 - 2.3 Red/Blue teams
 - 2.4 Bug bounty programs
3. Multi-layer system security testing
 - 3.1 Operating system exploits

- 3.2 Network penetration testing and tools
- 3.3 Web app penetration testing with OWASP and OSINT
- 3.4 Exploit development
- 4. Software testing
 - 4.1 Whitebox, blackbox and graybox testing
 - 4.2 Unit testing for security
 - 4.3 Fuzzing
 - 4.4 ISO/IEC 29119
- 5. Software verification
 - 5.1 Static code analysis
 - 5.2 Dynamic code analysis
 - 5.3 Peer review
 - 5.4 Formal verification
- 6. Cybersecurity Audits
 - 6.1 Self-assessments and third-party audits
 - 6.2 Risk-based approach to cybersecurity checks
 - 6.3 Auditing cybersecurity based on ISO/IEC 27001
 - 6.4 Toolset for automated audits

Literature

Compulsory Reading

Further Reading

- Graham, D. (2021). Ethical hacking: A hands-on introduction to breaking in. No Starch Press Incorporated.
- Keith Yorkston. (2021). Performance Testing: An ISTQB Certified Tester Foundation Level Specialist Certification Review: Vol. 1st ed . apress.
- Páez, F., & Kaschel, H. (2022). Design and Testing of a Computer Security Layer for the LIN Bus t. Sensors (14248220), 22(18), 6901–N.PAG.
- Li, H. (2022). Computer Security Issues and Legal System Based on Cloud Computing. Computational Intelligence & Neuroscience, 1–11.
- Shostack, A. (2014). Threat Modeling. Designing for Security. John Wiley & Sons, Hoboken, NJ. h
- Stallings, W., & Brown, L. (2018). Computer Security [electronic resource]: Principles and Practice (4th ed., global edition). Pearson Education, Limited.

Study Format Distance Learning

Study Format Distance Learning	Course Type Theory Course
--	-------------------------------------

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

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

Instructional Methods		
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	Learning Material <input checked="" type="checkbox"/> Course Book <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Slides	Exam Preparation <input checked="" type="checkbox"/> Practice Exam <input checked="" type="checkbox"/> Online Tests

Seminar: IT Security Tests

Course Code: DLMCSEEST02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSEEST01_E

Course Description

A good security architecture is a fine thing, but it is always better to test it than to find out too late that there was one more hole to patch. In this seminar, the student will complete a report on a security audit method. This can be a type of pentesting, red/blue team exercise or bug bounty program. Alternatively, the report can cover a vulnerability report created from a public bug bounty program. The intention is that the student has the opportunity to go in depth with an aspect of this subject.

Course Outcomes

On successful completion, students will be able to

- understand how bug bounty programs work.
- understand how to run a red/blue team or pentesting exercise.
- write a report showing aptitude in the subject.

Contents

- Testing security is just as important as implementing it. This seminar will address this topic with reports on a variety of subjects the student can choose from. The student will use current literature to research the topic and write a report on it. Possible topics can be based on tools in the areas of WWW pentesting, fuzzing, code security auditing. Or topics can be chosen from playbooks from red and blue teams. Or the student may choose to look into best practices for setting up and managing bug bounty programs.

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

- Kim, P. (2014): The Hacker Playbook: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA.
- Kim, P. (2015): The Hacker Playbook 2: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA.
- Kim, P. (2018): The Hacker Playbook 3: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA.
- Klein, T. (2011): A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security. No Starch Press, San Francisco, CA.
- McClure, S. / Scambray, J. / Kurtz, G. (2012): Hacking Exposed 7, McGraw-Hill, New York City, NY.
- The Zero-day Initiative blog: <https://www.zerodayinitiative.com/blog>

Study Format Distance Learning

Study Format Distance Learning	Course Type Seminar
--	-------------------------------

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

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

Instructional Methods		
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Learning Material <input checked="" type="checkbox"/> Slides	Exam Preparation <input checked="" type="checkbox"/> Guideline

Business Analyst

Modulcode: DLMDWWBA

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

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

Modulverantwortliche(r)

Prof. Dr. Peter Poensgen (Business Intelligence I) / Prof. Dr. Peter Poensgen (Projekt: Business Intelligence)

Kurse im Modul

- Business Intelligence I (DLMIWBI01)
- Projekt: Business Intelligence (DLMDWWBA01)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Business Intelligence I

- Studienformat "Fernstudium": Schriftliche Ausarbeitung; Fallstudie

Projekt: Business Intelligence

- Studienformat "Fernstudium": Portfolio

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls**Business Intelligence I**

- Motivation und Begriffsbildung
- Datenbereitstellung
- Data Warehouse
- Modellierung multidimensionaler Datenräume
- Analysesysteme
- Distribution und Zugriff
- Zukünftige Anwendungsgebiete von Business Intelligence

Projekt: Business Intelligence

Implementierung eines Business Intelligence Use Case. Eine aktuelle Themenliste befindet sich im Learning Management System.

Qualifikationsziele des Moduls**Business Intelligence I**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivationen und Anwendungsfälle für Business Intelligence sowie die Grundlagen von Business Intelligence zu verstehen.
- relevante Datentypen zu erläutern.
- Techniken und Methoden zur Modellierung und Verbreitung von Daten zu kennen und sich zu verdeutlichen.
- Techniken und Methoden zur Erzeugung und Speicherung von Informationen zu erläutern.
- geeignete Business-Intelligence-Methoden für die gegebenen Anforderungen auszuwählen.
- zukünftige Anwendungsgebiete von Business Intelligence zu erläutern.

Projekt: Business Intelligence

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Wissen über Business Intelligence-Methoden in die Praxis zu übertragen.
- die Eignung verschiedener Ansätze in Bezug auf die Projektaufgabe zu analysieren.
- kritisch über relevante Designentscheidungen nachzudenken.
- geeignete architektonische Entscheidungen zu treffen.
- ein Business Intelligence Use Case zu formulieren und zu implementieren.

Bezüge zu anderen Modulen im Studiengang

Baut auf Modulen aus den Bereichen Informatik & Software-Entwicklung sowie Data Science & Artificial Intelligence auf

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik

Business Intelligence I

Kurscode: DLMIWBI01

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

Beschreibung des Kurses

Bei Business Intelligence geht es um die Generierung von Informationen auf Basis von Betriebsdaten. Sie dient dazu, zielorientierte Managementpraktiken sowie die Optimierung relevanter Geschäftsaktivitäten zu ermöglichen. Dieser Kurs stellt Techniken, Methoden und Modelle für die Datenbereitstellung und die Erzeugung, Analyse und Verbreitung von Informationen vor und diskutiert sie.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivationen und Anwendungsfälle für Business Intelligence sowie die Grundlagen von Business Intelligence zu verstehen.
- relevante Datentypen zu erläutern.
- Techniken und Methoden zur Modellierung und Verbreitung von Daten zu kennen und sich zu verdeutlichen.
- Techniken und Methoden zur Erzeugung und Speicherung von Informationen zu erläutern.
- geeignete Business-Intelligence-Methoden für die gegebenen Anforderungen auszuwählen.
- zukünftige Anwendungsgebiete von Business Intelligence zu erläutern.

Kursinhalt

1. Motivation und Einführung
 - 1.1 Motivation und historische Entwicklung des Feldes
 - 1.2 Business Intelligence als Framework
2. Datenbereitstellung
 - 2.1 Operative und dispositive Systeme
 - 2.2 Das Data-Warehouse-Konzept
 - 2.3 Architekturvarianten
3. Data Warehouse
 - 3.1 Der ETL-Prozess
 - 3.2 DWH- und Data-Mart-Konzepte
 - 3.3 ODS und Metadaten

4. Modellierung multidimensionaler Datenräume
 - 4.1 Datenmodellierung
 - 4.2 OLAP-Würfel
 - 4.3 Physikalische Speicherkonzepte
 - 4.4 Sternenschema und Schneeflockenschema
 - 4.5 Historisierung
5. Analytische Systeme
 - 5.1 Freiform-Datenanalyse und OLAP
 - 5.2 Berichtssysteme
 - 5.3 Modellbasierte Analysesysteme
 - 5.4 Konzeptorientierte Systeme
6. Verteilung und Zugriff
 - 6.1 Informationsverteilung
 - 6.2 Informationszugang
7. Aktuelle und zukünftige Anwendungsfelder von Business Intelligence
 - 7.1 Mobile Business Intelligence
 - 7.2 Predictive and Prescriptive Analytics
 - 7.3 Künstliche Intelligenz
 - 7.4 Agile Business Intelligence

Literatur

Pflichtliteratur

Weiterführende Literatur

- Grossmann, W./Rinderle-Ma, S. (2015): Fundamentals of Business Intelligence. Springer, Berlin/Heidelberg.
- Kimball, R. (2013): The data warehouse toolkit: The definitive guide to dimensional modeling. 3rd edition, Wiley, Indianapolis, IN.
- Linstedt, D. / Olschimke, M. (2015): Building a scalable data warehouse with Data Vault 2.0. Morgan Kaufmann, Waltham, MA.
- Provost, F. (2013): Data science for business: What you need to know about data mining and data-analytic thinking. O'Reilly, Sebastopol, CA.
- Sherman, R. (2014): Business intelligence guidebook: From data integration to analytics. Morgan Kaufmann, Waltham, MA.
- Turban, E. et al (2010): Business intelligence. A managerial approach. 2nd edition, Prentice Hall, Upper Saddle River, NJ.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Online Tests <input checked="" type="checkbox"/> Prüfungsleitfaden

Projekt: Business Intelligence

Kurscode: DLMDWWBA01

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 5	Zugangsvoraussetzungen DLMIWBI01
---------------------	---	------------	----------------	--

Beschreibung des Kurses

In diesem Kurs vermitteln die Studenten Kenntnisse über Business Intelligence Ansätze und Methoden bei der Implementierung eines praxisnahen Business Analytical Use Case. Um dieses Ziel zu erreichen, müssen die Studenten die jeweilige Aufgabe genau betrachten und einen geeigneten Ansatz finden, indem sie verschiedene Lösungsstrategien und ihre Bestandteile analysieren, bewerten und vergleichen. Die gefundene Lösung muss dann umgesetzt werden, um zu einem laufenden Geschäftsanalyzesystem zu kommen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Wissen über Business Intelligence-Methoden in die Praxis zu übertragen.
- die Eignung verschiedener Ansätze in Bezug auf die Projektaufgabe zu analysieren.
- kritisch über relevante Designentscheidungen nachzudenken.
- geeignete architektonische Entscheidungen zu treffen.
- ein Business Intelligence Use Case zu formulieren und zu implementieren.

Kursinhalt

- Dieser zweite Kurs in der Fachrichtung Business Analyst zielt auf die praktische Umsetzung eines Business Intelligence Projekts ab. Die Studierenden können aus einer Liste von Projektthemen auswählen oder eigene Ideen einbringen.

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

- Kimball, R. (2013). The data warehouse toolkit: The definitive guide to dimensional modeling (3rd ed.). Indianapolis, IN: Wiley.
- Linstedt, D., & Olschimke, M. (2015). Building a scalable data warehouse with Data Vault 2.0. Waltham, MA: Morgan Kaufmann.
- Provost, F. (2013). Data science for business: What you need to know about data mining and data-analytic thinking. Sebastopol, CA: O'Reilly.
- Sherman, R. (2014). Business intelligence guidebook: From data integration to analytics. Waltham, MA: Morgan Kaufmann.
- Turban, E., Sharda, R., Delen, D., & King, D. (2010). Business intelligence. A managerial approach (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Projekt
-----------------------------------	---------------------------

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	Online Tests: Nein
Prüfungsleistung	Portfolio

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

Lehrmethoden		
Tutorielle Betreuung <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	Lernmaterial <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Prüfungsleitfaden

Continuous and Lifecycle Security

Module Code: DLMCSEECLS_E

Module Type see curriculum	Admission Requirements none	Study Level MA	CP 10	Student Workload 300 h
--------------------------------------	---------------------------------------	--------------------------	-----------------	----------------------------------

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

Module Coordinator

Nils Kannengießer (Cyber Resilience) / Prof. Dr. Stephan Spitz (Seminar: Applying Threat Intelligence)

Contributing Courses to Module

- Cyber Resilience (DLMCSEECLS01_E)
- Seminar: Applying Threat Intelligence (DLMCSEECLS02_E)

Module Exam Type

Module Exam

Split Exam

Cyber Resilience

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

Seminar: Applying Threat Intelligence

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

Weight of Module

see curriculum

Module Contents**Cyber Resilience**

- Cyber resilience
- DevSecOps
- Threat Intelligence
- Crisis Management
- Security Culture

Seminar: Applying Threat Intelligence

- Cyber resilience
- DevSecOps
- Threat Intelligence
- Crisis Management
- Security Culture

Learning Outcomes**Cyber Resilience**

On successful completion, students will be able to

- implement defense in depth and fault tolerance.
- work with resilience frameworks.
- use threat intelligence to design better resilience.
- use DevSecOps practices to improve resilience.
- manage crises that arise from attacks and corporate culture.

Seminar: Applying Threat Intelligence

On successful completion, students will be able to

- understand weaknesses in an organization's defenses.
- make recommendations on how to make the organization more resilient.
- utilize threat intelligence for secure application and systems design.

Links to other Modules within the Study Program

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

Links to other Study Programs of the University

All Master Programs in the IT & Technology fields

Cyber Resilience

Course Code: DLMCSEECLS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Even with state-of-the-art security controls in place, attacks will still be successful with enough persistence, and state actors and some criminals have shown a willingness to go that extra mile to penetrate their target. A resilient organization will have the monitoring and procedures in place and rapidly detect, triage and react to any attack. Furthermore, this organization will have enough fault tolerance so that an attack cannot affect the entire organization at the same time.

Course Outcomes

On successful completion, students will be able to

- implement defense in depth and fault tolerance.
- work with resilience frameworks.
- use threat intelligence to design better resilience.
- use DevSecOps practices to improve resilience.
- manage crises that arise from attacks and corporate culture.

Contents

1. Defense in depth
 - 1.1 The fallacy of complete security
 - 1.2 Byzantine fault tolerance
 - 1.3 Intrusion and fault detection
 - 1.4 Layers of protection
2. Design Principles
 - 2.1 Least Privilege
 - 2.2 Role and domain separation
 - 2.3 Revocation and Rollback
 - 2.4 Towards an anti-fragile organization
3. Fault tolerance
 - 3.1 Data protection and lifecycle
 - 3.2 Distributed and redundant data processing
 - 3.3 Applications of Blockchain technology

4. Frameworks
 - 4.1 NIST Cyber resilience engineering framework
 - 4.2 OODA-loop: Observe. Orient. Decide. Act.
5. Threat Intelligence
 - 5.1 Techniques, Tactics and Procedures
 - 5.2 Common weaknesses
 - 5.3 Threat Intelligence data
6. DevSecOps best practices
 - 6.1 Ephemeral processes
 - 6.2 Tiered data storage
 - 6.3 Continuous integration, testing and deployment with Canaries
 - 6.4 Availability zones for data and processes
 - 6.5 Avoiding complexity
7. Crisis management
 - 7.1 The Incident Response team
 - 7.2 Incident triage
 - 7.3 Communication
 - 7.4 Recovery planning and execution
 - 7.5 Postmortem
8. Organization and Culture
 - 8.1 Roles and responsibilities
 - 8.2 Security as a first-class citizen in an organization
 - 8.3 Influencing corporate culture
 - 8.4 Leadership buy-in

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

- Adkins, H. et al (2020): Building Secure and Reliable Systems. First Edition, O'Reilly Media, Newton, MA.
- Ross, R. et al (2019): Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-160 Volume 2. <https://doi.org/10.6028/NIST.SP.800-160v2>
- Ross, R. / McEvilley, M. / Oren, J. C. (2016): Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. <https://doi.org/10.6028/NIST.SP.800-160v1>

Study Format Distance Learning

Study Format Distance Learning	Course Type Theory Course
--	-------------------------------------

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

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

Instructional Methods		
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	Learning Material <input checked="" type="checkbox"/> Course Book <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Slides	Exam Preparation <input checked="" type="checkbox"/> Practice Exam <input checked="" type="checkbox"/> Online Tests

Seminar: Applying Threat Intelligence

Course Code: DLMCSEECLS02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Cyber resilience is the practice of accepting that security will never be 100% watertight but the ability to limit damage and quickly detect and respond to incidents is of utmost importance. In this seminar, we examine reports from past incidents and identify threat intelligence, in particular the Techniques, Tactics and Procedures of criminals, that help in identifying effective defenses.

Course Outcomes

On successful completion, students will be able to

- understand weaknesses in an organization's defenses.
- make recommendations on how to make the organization more resilient.
- utilize threat intelligence for secure application and systems design.

Contents

- With a given report, the student will research the incident and independently find threat intelligence reports and data relevant to the given incident. A report will then summarize the security issues responsible for the incident and make recommendations as to how the victim could become more resilient to such attacks. Specific incident reports will be provided by the tutor but proposals by the students can be considered.

Literature

Compulsory Reading

Further Reading

- Adkins, H. et al (2020): Building Secure and Reliable Systems. First Edition, O'Reilly Media, Inc.
- Mitre ATT&CK®: <https://attack.mitre.org/>
- OASIS Cyber Threat Intelligence: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
- Ross, R. et al (2019): Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-160 Volume 2. <https://doi.org/10.6028/NIST.SP.800-160v2>

Study Format Distance Learning

Study Format Distance Learning	Course Type Seminar
--	-------------------------------

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

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

Instructional Methods		
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Learning Material <input checked="" type="checkbox"/> Slides	Exam Preparation <input checked="" type="checkbox"/> Guideline

Data Science und Big Data Technologien

Modulcode: DLMCSEEDSBDT_D

Modultyp s. Curriculum	Zugangsvoraussetzungen keine	Niveau MA	CP 10	Zeitaufwand Studierende 300 h
----------------------------------	--	---------------------	-----------------	---

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

Modulverantwortliche(r)

Prof. Dr. Thomas Zöller (Data Science) / Prof. Dr. Christian Müller-Kett (Big-Data-Technologien)

Kurse im Modul

- Data Science (DLMDWDS01)
- Big-Data-Technologien (DLMDWBBDT01)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Data Science

- Studienformat "Fernstudium": Klausur, 90 Minuten

Big-Data-Technologien

- Studienformat "Fernstudium": Fachpräsentation

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls**Data Science**

- Einführung in die Data Science
- Anwendungsfälle und Leistungsbewertung
- Vorbehandlung von Daten
- Verarbeitung von Daten
- Ausgewählte mathematische Techniken
- Ausgewählte Techniken künstlicher Intelligenz

Big-Data-Technologien

- Datentypen und Datenquellen
- Datenbanken
- Moderne Speicher-Frameworks
- Datenverarbeitungs-Frameworks
- Aufbau skalierbarer Infrastrukturen

Qualifikationsziele des Moduls**Data Science**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Verwendung von Fällen zu bezeichnen und die Leistung von datengesteuerten Ansätzen zu bewerten.
- zu verstehen, wie Daten zur der Analyse vorverarbeitet werden.
- Typologien für Daten und Ontologien für die Wissensrepräsentation zu entwickeln.
- sich für geeignete mathematische Algorithmen zu entscheiden, um die Datenanalyse für eine bestimmte Aufgabe zu nutzen.
- den Wert, die Anwendbarkeit und die Grenzen der künstlichen Intelligenz für die Datenanalyse zu verstehen.

Big-Data-Technologien

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die verschiedenen Arten und Quellen von Daten zu identifizieren.
- verschiedene Datenbankkonzepte zu verstehen.
- neue Datenbankstrukturen aufzubauen.
- verschiedene Datenspeicher-Frameworks zu bewerten, bezogen auf die Projektanforderungen.
- zu analysieren, welches Datenformat für ein bestimmtes Projekt verwendet werden soll.
- eine verteilte Computerumgebung für ein bestimmtes Projekt zu erstellen.

Bezüge zu anderen Modulen im Studiengang

Baut auf Modulen aus dem Bereich Data Science & Artificial Intelligence auf.

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme aus dem Bereich IT & Technik.

Data Science

Kurscode: DLMDWDS01

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

Beschreibung des Kurses

Der Kurs Data Science bietet den Rahmen, um aus Daten Wert zu schaffen. Nach einer Einführung behandelt der Kurs, wie geeignete Anwendungsfälle identifiziert und die Leistung von datengesteuerten Methoden bewertet werden. Der Kurs behandelt Techniken für die technische Verarbeitung von Daten und stellt dann fortgeschrittene mathematische Techniken und ausgewählte Methoden der künstlichen Intelligenz vor, die zur Datenanalyse und für Vorhersagen verwendet werden.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Verwendung von Fällen zu bezeichnen und die Leistung von datengesteuerten Ansätzen zu bewerten.
- zu verstehen, wie Daten zur der Analyse vorverarbeitet werden.
- Typologien für Daten und Ontologien für die Wissensrepräsentation zu entwickeln.
- sich für geeignete mathematische Algorithmen zu entscheiden, um die Datenanalyse für eine bestimmte Aufgabe zu nutzen.
- den Wert, die Anwendbarkeit und die Grenzen der künstlichen Intelligenz für die Datenanalyse zu verstehen.

Kursinhalt

1. Einführung Data Science
 - 1.1 Überblick über Data Science
 - 1.2 Tätigkeiten der Data Science
 - 1.3 Datenquellen
 - 1.4 Deskriptive Statistik
2. Use Cases und Bewertung
 - 2.1 Data Science Use Cases (DSUCs)
 - 2.2 Bewertung
3. Datenvorverarbeitung
 - 3.1 Übermittlung von Daten
 - 3.2 Datenqualität, Bereinigung und Transformation

- 3.3 Datenvisualisierung
- 4. Verarbeitung von Daten
 - 4.1 Stufen der Datenverarbeitung
 - 4.2 Methoden und Arten der Datenverarbeitung
 - 4.3 Ausgabeformate der verarbeiteten Daten
- 5. Ausgewählte mathematische Techniken
 - 5.1 Hauptkomponentenanalyse
 - 5.2 Clusteranalyse
 - 5.3 Lineare Regression
 - 5.4 Zeitreihenanalyse
 - 5.5 Methoden zur Datentransformation
- 6. Ausgewählte Techniken der künstlichen Intelligenz
 - 6.1 Stütz-Vektor-Maschinen
 - 6.2 Künstliche neuronale Netze
 - 6.3 Weitere Ansätze

Literatur

Pflichtliteratur

Weiterführende Literatur

- Blobel, V./Lohrmann, E. (1998): Statistische und numerische Methoden der Datenanalyse. Teubner, Stuttgart/Leipzig. (Im Internet verfügbar).
- Bruce, A./Bruce, P. (2017): Practical Statistics for Data Scientists: 50 Essential Concepts. O'Reilly Publishers, Sebastopol (CA).
- Fahrmeir, L. et al. (2016): Statistik: Der Weg zur Datenanalyse. 8. Auflage, Springer Spektrum, Berlin/Heidelberg.
- Frochte, J. (2019): Maschinelles Lernen: Grundlagen und Algorithmen in Python. 2. Auflage, Carl Hanser, München.
- Liebowitz, J. (2014): Business analytics: An introduction. Auerbach Publications, Boca Raton (FL).
- Ng, A./Soo, K. (2018): Data Science – was ist das eigentlich?! Algorithmen des maschinellen Lernens verständlich erklärt. Springer, Berlin.
- Osterwalder, A./Pigneur, Y. (2011): Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer. Campus, Frankfurt/Main.
- VanderPlas, J. (2017): Data Science mit Python: Das Handbuch für den Einsatz von IPython, Jupyter, NumPy, Pandas, Matplotlib und Scikit-Learn. mitp, Frechen.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

Big-Data-Technologien

Kurscode: DLMDWBDT01

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

Beschreibung des Kurses

Daten werden oft als das "neue Öl" bezeichnet, der Rohstoff, aus dem Wert geschaffen wird. Um die Macht der Daten zu nutzen, müssen die Daten auf technischer Ebene gespeichert und verarbeitet werden. Dieser Kurs stellt die vier "Vs" von Daten sowie typische Datenquellen und -typen vor. Dieser Kurs behandelt dann, wie Daten in Datenbanken gespeichert werden. Besonderes Augenmerk wird auf Datenbankstrukturen und verschiedene Arten von Datenbanken gelegt, z.B. relationale, noSQL, NewSQL und Zeitreihen. Neben klassischen und modernen Datenbanken deckt dieser Kurs eine breite Palette von Speicher-Frameworks ab, wie z.B. verteilte Dateisysteme, Streaming und Query-Frameworks. Ergänzt wird dies durch eine ausführliche Diskussion der Datenspeicherformate, die von klassischen Ansätzen wie CSV und HDF5 bis hin zu moderneren Ansätzen wie Apache Arrow und Parquet reichen. Schließlich gibt dieser Kurs einen Überblick über verteilte Computerumgebungen, die auf lokalen Clustern, Cloud Computing-Einrichtungen und containerbasierten Ansätzen basieren.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die verschiedenen Arten und Quellen von Daten zu identifizieren.
- verschiedene Datenbankkonzepte zu verstehen.
- neue Datenbankstrukturen aufzubauen.
- verschiedene Datenspeicher-Frameworks zu bewerten, bezogen auf die Projektanforderungen.
- zu analysieren, welches Datenformat für ein bestimmtes Projekt verwendet werden soll.
- eine verteilte Computerumgebung für ein bestimmtes Projekt zu erstellen.

Kursinhalt

1. Datentypen und Datenquellen
 - 1.1 Die 4Vs der Daten: Volumen, Geschwindigkeit, Vielfalt, Wahrhaftigkeit.
 - 1.2 Datenquellen
 - 1.3 Datentypen
2. Datenbanken
 - 2.1 Datenbankstrukturen
 - 2.2 Einführung in SQL

- 2.3 Relationale Datenbanken
- 2.4 nonSQL, NewSQL Datenbanken
- 2.5 Zeitreihe DB
3. Moderne Datenspeicher-Frameworks
 - 3.1 Verteilte Dateisysteme
 - 3.2 Streaming-Frameworks
 - 3.3 Query-Frameworks
4. Datenverarbeitungs-Frameworks
 - 4.1 Traditionelle Datenaustauschformate
 - 4.2 Apache Arrow
 - 4.3 Apache Parquet
5. Aufbau skalierbarer Infrastrukturen
 - 5.1 Cluster-basierte Ansätze
 - 5.2 Container
 - 5.3 Cloud-basierte Ansätze

Literatur

Pflichtliteratur

Weiterführende Literatur

- Geisler, F. (2014). Datenbanken: Grundlagen und Design. Pearson.
- Kleppmann, M. (2017). Designing data-intensive applications. O'Reilly Media, Inc. Sebastopol, CA.
- Wiese, L. (2015). Advanced data management. De Gruyter.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	Online Tests: Ja
Prüfungsleistung	Fachpräsentation

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Online Tests <input checked="" type="checkbox"/> Prüfungsleitfaden

Automatisierungstechnik und Internet of Things

Modulcode: DLMDWWATIOT

Modultyp s. Curriculum	Zugangsvoraussetzungen keine	Niveau MA	CP 10	Zeitaufwand Studierende 300 h
----------------------------------	--	---------------------	-----------------	---

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

Modulverantwortliche(r)

Jacko Nudzor (Automatisierungstechnik) / Prof. Dr. Sebastian Lempert (Internet of Things)

Kurse im Modul

- Automatisierungstechnik (DLMDWAUTT01)
- Internet of Things (DLMDWWIOT01)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Automatisierungstechnik

- Studienformat "Fernstudium": Klausur, 90 Minuten

Internet of Things

- Studienformat "Fernstudium": Klausur, 90 Minuten

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls**Automatisierungstechnik**

- Mathematische Rahmenbedingungen für die formale Beschreibung von diskreten Ereignissystemen
- Analyse- und Bewertungsmethoden
- Simulation von diskreten Ereignissystemen
- Aufsichtskontrolle
- Fortgeschrittene Themen (Fehlerdiagnose, adaptive Überwachung, Optimierung)

Internet of Things

- Anwendungsfälle und Risiken für Verbraucher
- Business Use Cases und Risiken
- Sozialökonomische Fragen
- Ermöglichung von Technologien und Grundlagen der Vernetzung

Qualifikationsziele des Moduls

Automatisierungstechnik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wichtigsten Fragen im Zusammenhang mit der industriellen Automatisierung und insbesondere der Automatisierung von Industry 4.0 zu ermitteln.
- ein diskretes Ereignissystem formal mit Hilfe verschiedener mathematischer Modelle zu beschreiben.
- die Leistung eines Systems mit Hilfe von Formalismen und numerischen Simulationsansätzen zu analysieren.
- den besten Formalismus für ein gegebenes Designscenario auszuwählen und Anforderungen zu formulieren.
- Entwurf und Implementierung eines aufsichtsrechtlichen Controllers zur Erfüllung der Anforderungen zu erstellen.
- fortgeschrittene Themen im Zusammenhang mit Industry 4.0 Industrieautomation zu verstehen.

Internet of Things

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine breite Palette von Anwendungsfällen für das Internet der Dinge (IoT) zu unterscheiden und zu diskutieren.
- die verschiedenen Perspektiven des IoT zu verstehen und zu reflektieren.
- verschiedene Techniken anzuwenden, um Produkte aus dem Internet der Dinge zu entwickeln.
- Bewertung und Identifizierung geeigneter IoT-Kommunikationstechnologien und -Standards gemäß den gegebenen IoT-Produktanforderungen vorzunehmen.
- die jeweiligen theoretischen Grundlagen zu reflektieren, verschiedene Ansätze zu bewerten und geeignete Ansätze für praktische Fragen und Fälle anzuwenden.

Bezüge zu anderen Modulen im Studiengang

Ist Grundlage für alle weiteren Module aus den Bereichen Ingenieurwissenschaften und Informatik & Software-Entwicklung

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik

Automatisierungstechnik

Kurscode: DLMDWAUTT01

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

Beschreibung des Kurses

Produktionssysteme können als diskrete Ereignissysteme beschrieben werden, bei denen die Entwicklung durch das Auftreten von Ereignissen gekennzeichnet ist. Im Zeitalter von Industry 4.0 und der hochflexiblen Fertigung besteht die Notwendigkeit, angemessene Mittel für die Modellierung, Analyse, Konstruktion und Steuerung flexibler Produktionsumgebungen bereitzustellen. Dieser Kurs stellt mehrere Modellierungsansätze für die mathematische Beschreibung diskreter Ereignissysteme wie Automata, Petri-Netze und Markov-Prozesse vor. Jeder Ansatz wird in Theorie und Praxis mit Beispielen aus der Industrie vorgestellt. Die Ansätze sind in der Logik gruppiert - wobei nur die logische Abfolge der Ereignisse die Entwicklung bestimmt - und zeitlich begrenzt, wobei auch der Zeitplan der Ereignisse eine wichtige Rolle spielt. Obwohl einfache diskrete Ereignissysteme mathematisch analysiert werden können, benötigen komplexe Systeme die Unterstützung der Computersimulation. Die Hauptthemen der Simulation von diskreten Ereignissystemen werden behandelt. Der letzte Teil dieses Kurses stellt das Konzept der Aufsichtskontrolle vor, das darauf abzielt, die Eigenschaften eines bestimmten Systems zu ändern, um bestimmte Verhaltensweisen zu verbessern und definierte Designspezifikationen zu erfüllen. Die Aufsichtskontrolle wird sowohl von der theoretischen Praxis als auch von der Praxis angesprochen und beschreibt, wie sie in einem modernen industriellen Umfeld umgesetzt werden kann. Der Kurs schließt mit der Diskussion interessanter Anwendungen für Modellierungs- und Designansätze ab, z.B. bei der Modellierung und Analyse einer industriellen Produktionseinheit. Zusätzliche Gespräche zu Themen wie Fehlerdiagnose, dezentrale und verteilte Überwachung, Optimierung und adaptive Überwachung stellen eine kontingente Verbindung zwischen der klassischen Industrieautomation und der aktuellen, (großen) datengesteuerten, flexiblen Industry 4.0 Advanced Industrial Automation dar.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die wichtigsten Fragen im Zusammenhang mit der industriellen Automatisierung und insbesondere der Automatisierung von Industry 4.0 zu ermitteln.
- ein diskretes Ereignissystem formal mit Hilfe verschiedener mathematischer Modelle zu beschreiben.
- die Leistung eines Systems mit Hilfe von Formalismen und numerischen Simulationsansätzen zu analysieren.
- den besten Formalismus für ein gegebenes Designszenario auszuwählen und Anforderungen zu formulieren.
- Entwurf und Implementierung eines aufsichtsrechtlichen Controllers zur Erfüllung der Anforderungen zu erstellen.
- fortgeschrittene Themen im Zusammenhang mit Industry 4.0 Industrieautomation zu verstehen.

Kursinhalt

1. Einführung in die Produktionssysteme
 - 1.1 Was sind Produktionssysteme?
 - 1.2 Industrielle Überwachung und Kontrolle
 - 1.3 Herausforderungen
 - 1.4 Trends
2. Automaten
 - 2.1 Voraussetzungen
 - 2.2 Deterministische endliche Automaten
 - 2.3 Nichtdeterministische endliche Automaten
 - 2.4 Eigenschaften
3. Petri-Netze
 - 3.1 Voraussetzungen
 - 3.2 Modellierungssysteme
 - 3.3 Eigenschaften
 - 3.4 Analysemethoden
4. Zeitbewertete Modelle
 - 4.1 Zeitbewertete Automaten
 - 4.2 Markov-Prozesse
 - 4.3 Warteschlangentheorie
 - 4.4 Zeitbewertete Petri-Netze

5. Simulation von diskreten Ereignissystemen
 - 5.1 Grundlegende Konzepte
 - 5.2 Funktionsprinzipien
 - 5.3 Performanceanalyse
 - 5.4 Software-Tools
6. Supervisory Control
 - 6.1 Grundlegendes Konzept
 - 6.2 Technische Daten
 - 6.3 Synthese
 - 6.4 Performanceanalyse
 - 6.5 Implementierung
7. Anwendungen
 - 7.1 Überwachung von Produktionssystemen
 - 7.2 Kontrolle und Diagnose von Fehlern
 - 7.3 Verteilte und dezentralisierte Überwachung
 - 7.4 Modellgestützte Optimierung von Produktionssystemen
 - 7.5 Adaptiv überwachte Steuerung

Literatur

Pflichtliteratur

Weiterführende Literatur

- Cassandras, C. G., & Lafortune, S. (2009). Introduction to discrete event systems. Springer.
- Hooley, G., Nicoulaud, B., Rudd, J. M., & Piercy, N. (2019). Marketing strategy and competitive positioning. Pearson.
- Kaplan, R., Norton, D., & Rugelsjoen, B. (2010). Managing alliances with the balanced scorecard. *Harvard Business Review*, 88(1/2), 114–120.
- Linz, P. (2006). An introduction to formal languages and automata. Jones & Bartlett Learning.
- Reisig, W. (2013). Understanding Petri nets: Modeling techniques, analysis methods, case studies. Springer.
- Stewart, J. B. (2013, October 14). The collapse: How a top legal firm destroyed itself. *The New Yorker*.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Skript <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Folien	<input checked="" type="checkbox"/> Musterklausur <input checked="" type="checkbox"/> Online Tests

Internet of Things

Kurscode: DLMDWWIOT01

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

Beschreibung des Kurses

Das Internet der Dinge (IoT), einst eine grobe Vision, ist heute auf breiter Basis Realität geworden. Es gibt eine Vielzahl von Geräten und Dienstleistungen, die sowohl Verbrauchern als auch Unternehmen zur Verfügung stehen. Von intelligenten Häusern bis hin zu intelligenten Städten, von intelligenten Geräten bis hin zu intelligenten Fabriken - das Internet der Dinge beeinflusst Technologien unser Leben und unsere Umwelt. Dieser Kurs folgt einem Top-Down-Ansatz und diskutiert eine breite Palette von Aspekten, die mit dem Internet der Dinge verbunden sind. Es beginnt mit Use Cases und Risiken aus der Sicht von Kunden und Unternehmen und endet mit einer technischen Grundlage des Internet der Dinge. Um die technische Perspektive anzugehen, wird eine Reihe von Techniken vorgeschlagen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine breite Palette von Anwendungsfällen für das Internet der Dinge (IoT) zu unterscheiden und zu diskutieren.
- die verschiedenen Perspektiven des IoT zu verstehen und zu reflektieren.
- verschiedene Techniken anzuwenden, um Produkte aus dem Internet der Dinge zu entwickeln.
- Bewertung und Identifizierung geeigneter IoT-Kommunikationstechnologien und -Standards gemäß den gegebenen IoT-Produktanforderungen vorzunehmen.
- die jeweiligen theoretischen Grundlagen zu reflektieren, verschiedene Ansätze zu bewerten und geeignete Ansätze für praktische Fragen und Fälle anzuwenden.

Kursinhalt

1. Einführung in das Internet der Dinge
 - 1.1 Grundlagen und Motivation
 - 1.2 Potenziale und Herausforderungen
2. Soziale und wirtschaftliche Relevanz
 - 2.1 Innovationen für Verbraucher:innen
 - 2.2 Innovationen für die Industrie
 - 2.3 Auswirkungen der Digitalisierung auf Mensch und Arbeitsumfeld
 - 2.4 Datenschutz und IT-Sicherheit

3. Architekturen des Internets der Dinge
 - 3.1 Komponenten einer IoT-Gesamtsystemarchitektur
 - 3.2 Edge, Fog und Cloud Computing
 - 3.3 Grundlagen zu IoT-Hardware-Plattformen
 - 3.4 Beliebte IoT-Hardware-Plattformen
 - 3.5 Auto-ID-Technologien als IoT-Basistechnologien
4. Kommunikationsstandards und -technologien
 - 4.1 Grundlagen zu Kommunikationsprotokollen
 - 4.2 Kommunikationsprotokolle für das IoT und die Industrie 4.0
 - 4.3 Netzwerktopologien
 - 4.4 Nachrichtenübermittlungsmuster
 - 4.5 Auswahlkriterien für IoT-Kommunikationsprotokolle
5. Datenspeicherung und -verarbeitung
 - 5.1 Complex Event Processing
 - 5.2 Maschinelles Lernen (ML)
 - 5.3 Kombination von CEP und ML

Literatur

Pflichtliteratur

Weiterführende Literatur

- Chaouchi, H. (2013). The internet of things: Connecting objects. London: Wiley.
- Greengard, S. (2015). The internet of things. Cambridge, MA: MIT Press.
- Kellmerit, D., & Obodovski, D. (2013). The silent intelligence: The internet of things. San Francisco, CA: DND Ventures.
- Slama, D., Puhmann, F., Morrish, J., & Bhatnagar, R. M. (2016). Enterprise IoT: Strategies and best practices for connected products and services. Beijing, Boston, Farnham, Sebastopol, Tokyo: O'Reilly.
- Weber, R. H., & Weber, R. (2010). Internet of things: Legal perspectives. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

Künstliche Intelligenz

Modulcode: DLMIMWKI_D

Modultyp s. Curriculum	Zugangsvoraussetzungen keine	Niveau MA	CP 10	Zeitaufwand Studierende 300 h
----------------------------------	--	---------------------	-----------------	---

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

Modulverantwortliche(r)

Prof. Dr. Thomas Zöller (Künstliche Intelligenz) / Dr. Maja Popovic (Seminar: Künstliche Intelligenz und Gesellschaft)

Kurse im Modul

- Künstliche Intelligenz (DLMAIAI01_D)
- Seminar: Künstliche Intelligenz und Gesellschaft (DLMAISAI01_D)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Künstliche Intelligenz

- Studienformat "Fernstudium": Klausur, 90 Minuten

Seminar: Künstliche Intelligenz und Gesellschaft

- Studienformat "Fernstudium": Schriftliche Ausarbeitung; Seminararbeit

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls**Künstliche Intelligenz**

- Geschichte der KI
- KI-Anwendungsbereiche
- Expertensysteme
- Neurowissenschaften
- Moderne KI-Systeme

Seminar: Künstliche Intelligenz und Gesellschaft

In diesem Seminar werden die Studierenden über die aktuellen gesellschaftlichen und politischen Implikationen der künstlichen Intelligenz nachdenken. Zu diesem Zweck werden relevante Themen in Form von Artikeln vorgestellt, die von den Studierenden in einem schriftlichen Aufsatz kritisch bewertet werden.

Qualifikationsziele des Moduls**Künstliche Intelligenz**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sich einen Überblick über die historischen Entwicklungen im Bereich der künstlichen Intelligenz zu verschaffen.
- die verschiedenen Anwendungsbereiche der künstlichen Intelligenz zu analysieren.
- Expertensysteme zu verstehen.
- Prolog auf einfache Expertensysteme anzuwenden.
- das Gehirn und die kognitiven Prozesse aus neurowissenschaftlicher Sicht zu verstehen.
- moderne Entwicklungen in der künstlichen Intelligenz zu verstehen.

Seminar: Künstliche Intelligenz und Gesellschaft

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ausgewählte aktuelle gesellschaftliche Themen und Fragestellungen der künstlichen Intelligenz zu nennen.
- den Einfluss und die Auswirkungen der künstlichen Intelligenz auf gesellschaftliche, wirtschaftliche und politische Themen zu erklären.
- theoretisch erworbenes Wissen auf reale Fälle zu übertragen.
- ein ausgewähltes Thema in Form eines schriftlichen Aufsatzes wissenschaftlich zu behandeln.
- aktuelle gesellschaftliche und politische Fragen, die sich aus den jüngsten Fortschritten in der Methodik der künstlichen Intelligenz ergeben, kritisch zu hinterfragen und zu diskutieren.
- eigene Problemlösungsfähigkeiten und -prozesse durch Reflexion über die möglichen Auswirkungen ihrer zukünftigen Tätigkeit im Bereich der künstlichen Intelligenz zu entwickeln.

Bezüge zu anderen Modulen im Studiengang

Baut auf Modulen aus dem Bereich Data Science & Artificial Intelligence auf

Bezüge zu anderen Studiengängen der Hochschule

Alle Master-Programme im Bereich IT & Technik

Künstliche Intelligenz

Kurscode: DLMAIAI01_D

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

Beschreibung des Kurses

Die Suche nach künstlicher Intelligenz hat das Interesse der Menschheit seit vielen Jahrzehnten bewegt und wird seit den 1960er Jahren rege beforscht. Dieser Kurs gibt einen detaillierten Überblick über die historischen Entwicklungen, Erfolge und Rückschläge in der KI sowie die Entwicklung und den Einsatz von Expertensystemen in frühen KI-Systemen. Um kognitive Prozesse zu verstehen, wird der Kurs einen kurzen Überblick über das biologische Gehirn und (menschliche) kognitive Prozesse geben und sich dann auf die Entwicklung moderner KI-Systeme konzentrieren, die durch die jüngsten Entwicklungen im Bereich der Hard- und Software vorangetrieben werden. Besonderes Augenmerk liegt auf der Diskussion der Entwicklung "schmaler KI"-Systeme für spezifische Anwendungsfälle im Vergleich zur Schaffung allgemeiner künstlicher Intelligenz. Der Kurs gibt einen Überblick über ein breites Spektrum potenzieller Anwendungsbereiche der künstlichen Intelligenz, darunter Industriebereiche wie autonomes Fahren und Mobilität, Medizin, Finanzen, Einzelhandel und Produktion.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sich einen Überblick über die historischen Entwicklungen im Bereich der künstlichen Intelligenz zu verschaffen.
- die verschiedenen Anwendungsbereiche der künstlichen Intelligenz zu analysieren.
- Expertensysteme zu verstehen.
- Prolog auf einfache Expertensysteme anzuwenden.
- das Gehirn und die kognitiven Prozesse aus neurowissenschaftlicher Sicht zu verstehen.
- moderne Entwicklungen in der künstlichen Intelligenz zu verstehen.

Kursinhalt

1. Geschichte der Künstlichen Intelligenz
 - 1.1 Historische Entwicklung
 - 1.2 KI-Winter
 - 1.3 Bemerkenswerte Fortschritte auf dem Gebiet der Künstlichen Intelligenz
2. Frühe Systeme der Künstlichen Intelligenz
 - 2.1 Überblick über Expertensysteme
 - 2.2 Einführung in Prolog

- 2.3 Mustererkennung und maschinelles Lernen (ML)
 - 2.4 Anwendungsfälle
3. Neurowissenschaft und Kognitionswissenschaft
 - 3.1 Neurowissenschaft und das menschliche Gehirn
 - 3.2 Kognitionswissenschaft
 - 3.3 Zusammenhänge zwischen Neurowissenschaft, Kognitionswissenschaft und Künstlicher Intelligenz
4. Moderne KI-Systeme
 - 4.1 Neueste Entwicklungen bei Hardware und Software
 - 4.2 Enge und allgemeine Künstliche Intelligenz
 - 4.3 Sprachverarbeitung und Computer Vision
5. Anwendungen der Künstlichen Intelligenz
 - 5.1 Mobilität und autonome Fahrzeuge
 - 5.2 Personalisierte Medizin
 - 5.3 FinTech
 - 5.4 Handel und Industrie

Literatur

Pflichtliteratur

Weiterführende Literatur

- Ertel, W. (2021). Grundkurs Künstliche Intelligenz: Eine praxisorientierte Einführung (5. Aufl.). Springer Vieweg.
- Russell, S. & Norvig, P. (2022). Artificial Intelligence. A Modern Approach (4. Aufl.). Pearson Education.
- Lucas, P.J.F & Van der Gaag, L. (1991). Principles of Expert sSystems. Addison Wesley .
- Ward, J. (2019). The student's guide to cognitive neuroscience (4. Aufl.). Taylor & Francis Group.
- Frankish, K & Ramsey, W.M. (Hg.) (2012). The Cambridge hHandbook of Cognitive Science. Cambridge University Press.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Theoriekurs
-----------------------------------	-------------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung	Lernmaterial	Prüfungsvorbereitung
<input checked="" type="checkbox"/> Course Feed	<input checked="" type="checkbox"/> Skript	<input checked="" type="checkbox"/> Musterklausur
<input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	<input checked="" type="checkbox"/> Video	<input checked="" type="checkbox"/> Online Tests
<input checked="" type="checkbox"/> Recorded Live Sessions	<input checked="" type="checkbox"/> Folien	

Seminar: Künstliche Intelligenz und Gesellschaft

Kurscode: DLMAISAI01_D

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

Beschreibung des Kurses

Im laufenden Jahrzehnt wurden auf dem Gebiet der künstlichen Intelligenz beeindruckende Fortschritte erzielt. Verschiedene kognitive Aufgaben wie die Objekterkennung in Bild und Video, die Verarbeitung natürlicher Sprache, die Spielstrategie und das autonome Fahren und die Robotik werden heute von Maschinen auf einem noch nie dagewesenen Niveau ausgeführt. In diesem Kurs werden einige der gesellschaftlichen, wirtschaftlichen und politischen Auswirkungen dieser Entwicklungen untersucht.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ausgewählte aktuelle gesellschaftliche Themen und Fragestellungen der künstlichen Intelligenz zu nennen.
- den Einfluss und die Auswirkungen der künstlichen Intelligenz auf gesellschaftliche, wirtschaftliche und politische Themen zu erklären.
- theoretisch erworbenes Wissen auf reale Fälle zu übertragen.
- ein ausgewähltes Thema in Form eines schriftlichen Aufsatzes wissenschaftlich zu behandeln.
- aktuelle gesellschaftliche und politische Fragen, die sich aus den jüngsten Fortschritten in der Methodik der künstlichen Intelligenz ergeben, kritisch zu hinterfragen und zu diskutieren.
- eigene Problemlösungsfähigkeiten und -prozesse durch Reflexion über die möglichen Auswirkungen ihrer zukünftigen Tätigkeit im Bereich der künstlichen Intelligenz zu entwickeln.

Kursinhalt

- Das Seminar behandelt aktuelle Themen zu den gesellschaftlichen Auswirkungen der künstlichen Intelligenz. Alle Teilnehmenden erstellen eine Seminararbeit zu einem zugewiesenen Thema.

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

- Boddington, P. (2017): Towards a code of ethics for artificial intelligence. 1st ed., Springer International Publishing, New York, NY.
- Bostrom, N. (2016): Superintelligence: Paths, dangers, strategies. Oxford University Press, Oxford.
- Tegmark, M. (2018): Life 3.0: Being human in the age of artificial intelligence. Penguin, New York, NY.
- Wachter-Boettcher, S. (2017): Technically wrong: Sexist apps, biased algorithms, and other threats of toxic tech. W. W. Norton & Company, New York, NY.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Seminar
-----------------------------------	---------------------------

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

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

Lehrmethoden		
Tutorielle Betreuung <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint	Lernmaterial <input checked="" type="checkbox"/> Folien	Prüfungsvorbereitung <input checked="" type="checkbox"/> Prüfungsleitfaden

AI and Mastering AI Prompting

Module Code: DLMEAIMAIP

Module Type see curriculum	Admission Requirements none	Study Level MA	CP 10	Student Workload 300 h
--------------------------------------	---------------------------------------	--------------------------	-----------------	----------------------------------

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

Module Coordinator

Prof. Dr. Claudia Heß (Artificial Intelligence) / Prof. Dr. Gissel Velarde Perez (Project: AI Excellence with Creative Prompting Techniques)

Contributing Courses to Module

- Artificial Intelligence (DLMAIAI01)
- Project: AI Excellence with Creative Prompting Techniques (DLMPAIECPT01)

Module Exam Type

Module Exam

Split Exam

Artificial Intelligence

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

Project: AI Excellence with Creative Prompting Techniques

- Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Artificial Intelligence

- History of AI
- Expert Systems
- Neuroscience
- Modern AI Systems
- AI Application Areas

Project: AI Excellence with Creative Prompting Techniques

In this module, students delve into the world of generative AI applications, creating AI-generated content such as text, images, and videos. They learn to design, analyze, and evaluate different prompting techniques in these systems and apply them within their respective fields of study.

Learning Outcomes

Artificial Intelligence

On successful completion, students will be able to

- remember the historical developments in the field of artificial intelligence.
- analyze the different application areas of artificial intelligence.
- comprehend expert systems.
- apply Prolog to simple expert systems.
- comprehend the brain and cognitive processes from a neuro-scientific point of view.
- understand modern developments in artificial intelligence.

Project: AI Excellence with Creative Prompting Techniques

On successful completion, students will be able to

- comprehend and implement various prompting techniques in generative AI applications.
- analyze, assess, and combine different prompt techniques for various expected AI outputs.
- implement ethical considerations into the design and execution of various generative AI applications.
- design, implement, and refine effective prompts and their combinations for real-world scenarios through various hands-on exercises.
- showcase creative and innovative thinking and reasoning in the application of advanced prompting techniques to solve multidimensional problems in their specialized area of study.

Links to other Modules within the Study Program

This module is similar to other modules in the field of Data Science & Artificial Intelligence

Links to other Study Programs of the University

All Master Programs in the IT & Technology field

Artificial Intelligence

Course Code: DLMAIAI01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The quest for artificial intelligence has captured humanity's interest for many decades and has been an active research area since the 1960s. This course will give a detailed overview of the historical developments, successes, and set-backs in AI, as well as the development and use of expert systems in early AI systems. In order to understand cognitive processes, the course will give a brief overview of the biological brain and (human) cognitive processes and then focus on the development of modern AI systems fueled by recent developments in hard- and software. Particular focus will be given to discussion of the development of "narrow AI" systems for specific use cases vs. the creation of general artificial intelligence. The course will give an overview of a wide range of potential application areas in artificial intelligence, including industry sectors such as autonomous driving and mobility, medicine, finance, retail, and manufacturing.

Course Outcomes

On successful completion, students will be able to

- remember the historical developments in the field of artificial intelligence.
- analyze the different application areas of artificial intelligence.
- comprehend expert systems.
- apply Prolog to simple expert systems.
- comprehend the brain and cognitive processes from a neuro-scientific point of view.
- understand modern developments in artificial intelligence.

Contents

1. History of AI
 - 1.1 Historical Developments
 - 1.2 AI Winter
 - 1.3 Notable Advances in AI
2. Expert Systems
 - 2.1 Overview Over Expert Systems
 - 2.2 Introduction to Prolog
3. Neuroscience
 - 3.1 The (Human) Brain

3.2 Cognitive Processes

4. Modern AI Systems

4.1 Recent Developments in Hard- and Software

4.2 Narrow vs General AI

4.3 NLP and Computer Vision

5. AI Application Areas

5.1 Autonomous Vehicles & Mobility

5.2 Personalized Medicine

5.3 FinTech

5.4 Retail & Industry

Literature

Compulsory Reading

Further Reading

- Chowdhary, K. R. (2020). Fundamentals of Artificial Intelligence. Springer India.
- Russell, S. & Norvig, P. (2022). Artificial intelligence. A modern approach (4th ed.). Pearson Education.
- Ward, J. (2020). The student's guide to cognitive neuroscience. (4th ed.). Taylor & Francis Group.

Study Format Distance Learning

Study Format Distance Learning	Course Type Theory Course
--	-------------------------------------

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

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

Instructional Methods		
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	Learning Material <input checked="" type="checkbox"/> Course Book <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Slides	Exam Preparation <input checked="" type="checkbox"/> Practice Exam <input checked="" type="checkbox"/> Online Tests

Study Format myStudies

Study Format myStudies	Course Type Theory Course
----------------------------------	-------------------------------------

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

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

Instructional Methods		
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	Learning Material <input checked="" type="checkbox"/> Course Book <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Slides	Exam Preparation <input checked="" type="checkbox"/> Practice Exam <input checked="" type="checkbox"/> Online Tests

Project: AI Excellence with Creative Prompting Techniques

Course Code: DLMPAIECPT01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

In this course, students explore the exciting world of prompting in various generative AI applications. They involve themselves in hands-on exercises that combine various prompting techniques to create new AI-generated content, including text, images, and videos. Through these exercises, students learn how to effectively use, analyze, combine, and assess these systems within their specialized fields of study.

Course Outcomes

On successful completion, students will be able to

- comprehend and implement various prompting techniques in generative AI applications.
- analyze, assess, and combine different prompt techniques for various expected AI outputs.
- implement ethical considerations into the design and execution of various generative AI applications.
- design, implement, and refine effective prompts and their combinations for real-world scenarios through various hands-on exercises.
- showcase creative and innovative thinking and reasoning in the application of advanced prompting techniques to solve multidimensional problems in their specialized area of study.

Contents

- In this course, students engage in a practical application of a generative AI use case by choosing from the options provided in the extensive supplementary guide. The course presents practical examples as study materials and exercises with both individual and combined prompting techniques for open-source text, image, and video generation use cases. The exercises are crafted to inspire and lead students in executing their distinct generative AI use case work and provide guidance on describing the use case and selecting a mixture of prompting techniques. Additionally, students are led to critically evaluate the design, implementation, and the outcomes 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>
- Epstein, Z., Hertzmann, A., Herman, L., Mahari, R., Frank, M. R., Groh, M., Schroeder, H., Smith, A., Akten, M., Fjeld, J., Farid, H., Leach, N., Pentland, A. S., & Russakovsky, O. (2023). Art and the science of generative AI: A deeper dive. arXiv. <https://arxiv.org/pdf/2306.04141.pdf>
- Gozalo-Brizuela, R., & Garrido-Merchán, E. C. (2023). A survey of generative AI applications. arXiv. <https://arxiv.org/pdf/2306.02781.pdf>
- Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E. H., Le., Q. V., & Zhou, D. (2023). Chain-of-thought prompting elicit reasoning in large language models. arXiv. <https://arxiv.org/pdf/2201.11903.pdf>

Study Format Distance Learning

Study Format Distance Learning	Course Type Project
--	-------------------------------

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

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

Instructional Methods	
Tutorial Support <input checked="" type="checkbox"/> Course Feed <input checked="" type="checkbox"/> Intensive Live Sessions/Learning Sprint <input checked="" type="checkbox"/> Recorded Live Sessions	Exam Preparation <input checked="" type="checkbox"/> Guideline

4. Semester

Masterarbeit

Modulcode: MMTH

Modultyp s. Curriculum	Zugangsvoraussetzungen Gemäß Studien- und Prüfungsordnung	Niveau MA	CP 30	Zeitaufwand Studierende 900 h
----------------------------------	---	---------------------	-----------------	---

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

Modulverantwortliche(r)

Studiengangsleiter (SGL) (Masterarbeit) / Studiengangsleiter (SGL) (Kolloquium)

Kurse im Modul

- Masterarbeit (MMTH01)
- Kolloquium (MMTH02)

Art der Prüfung(en)

Modulprüfung

Teilmodulprüfung

Masterarbeit

- Studienformat "Fernstudium": Schriftliche Ausarbeitung; Masterarbeit

Kolloquium

- Studienformat "Fernstudium": Kolloquium

Anteil der Modulnote an der Gesamtnote

s. Curriculum

<p>Lehrinhalt des Moduls</p> <p>Masterarbeit</p> <ul style="list-style-type: none"> ▪ Masterarbeit <p>Kolloquium</p> <ul style="list-style-type: none"> ▪ Kolloquium zur Masterarbeit 	
<p>Qualifikationsziele des Moduls</p> <p>Masterarbeit</p> <p>Nach erfolgreichem Abschluss sind die Studierenden in der Lage,</p> <ul style="list-style-type: none"> ▪ 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 Masterarbeit angemessene Erfassung und Analyse vorhandener (Forschungs-)Literatur vorzunehmen. ▪ eine ausführliche schriftliche Ausarbeitung unter Einhaltung wissenschaftlicher Methoden zu erstellen. <p>Kolloquium</p> <p>Nach erfolgreichem Abschluss sind die Studierenden in der Lage,</p> <ul style="list-style-type: none"> ▪ eine Problemstellung aus ihrem Studienschwerpunkt unter Beachtung akademischer Präsentations- und Kommunikationstechniken vorzustellen. ▪ das in der Masterarbeit gewählte wissenschaftliche und methodisch Vorgehen reflektiert darzustellen. ▪ themenbezogene Fragen von Fachexperten (Gutachter der Masterarbeit) aktiv zu beantworten. 	
<p>Bezüge zu anderen Modulen im Studiengang</p> <p>Alle Module im Masterprogramm</p>	<p>Bezüge zu anderen Studiengängen der Hochschule</p> <p>Alle Masterprogramme im Fernstudium</p>

Masterarbeit

Kurscode: MMTH01

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 27	Zugangsvoraussetzungen gemäß Studien- und Prüfungsordnung
---------------------	---	------------	-----------------	---

Beschreibung des Kurses

Ziel und Zweck der Masterarbeit 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 Masterarbeit kann eine praktisch-empirische oder aber theoretisch-wissenschaftliche Problemstellung sein. Studierende sollen unter Beweis stellen, dass sie eigenständig unter fachlich-methodischer Anleitung eines akademischen Betreuers eine ausgewählte Problemstellung mit wissenschaftlichen Methoden analysieren, kritisch bewerten und Lösungsvorschläge erarbeiten können. Das von dem Studierenden zu wählende Thema aus dem jeweiligen Studienschwerpunkt soll nicht nur die erworbenen wissenschaftlichen Kompetenzen unter Beweis stellen, sondern auch das akademische Wissen des Studierenden vertiefen und abrunden, um seine Berufsfähigkeiten und -fertigkeiten optimal auf die Bedürfnisse des zukünftigen Tätigkeitsfeldes auszurichten.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Anwendung der fachlichen und methodischen Kompetenzen, die sie im Studium erworben haben, zu bearbeiten.
- eigenständig – unter fachlich-methodischer Anleitung eines akademischen Betreuers – ausgewählte Aufgabenstellungen mit wissenschaftlichen Methoden zu analysieren, kritisch zu bewerten sowie entsprechende Lösungsvorschläge zu erarbeiten.
- eine dem Thema der Masterarbeit angemessene Erfassung und Analyse vorhandener (Forschungs-)Literatur vorzunehmen.
- eine ausführliche schriftliche Ausarbeitung unter Einhaltung wissenschaftlicher Methoden zu erstellen.

Kursinhalt

- Im Rahmen der Masterarbeit muss 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

Studienformat Fernstudium

Studienform Fernstudium	Kursart Thesis-Kurs
-----------------------------------	-------------------------------

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	Online Tests: Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Masterarbeit

Zeitaufwand Studierende					
Selbststudium 810 h	Präsenzstudium 0 h	Tutorium/ Tutorielle Betreuung 0 h	Selbstüberprüfung 0 h	Praxisanteil 0 h	Gesamt 810 h

Lehrmethoden
Die Studierenden schreiben ihre Masterarbeit eigenständig unter der methodischen und wissenschaftlicher Anleitung eine akademischen Betreuers.

Kolloquium

Kurscode: MMTH02

Niveau MA	Kurs- und Prüfungssprache Deutsch	SWS	CP 3	Zugangsvoraussetzungen gemäß Studien- und Prüfungsordnung
---------------------	---	------------	----------------	---

Beschreibung des Kurses

Das Kolloquium wird nach Einreichung der Masterarbeit 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, und 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 Masterarbeit gewählte wissenschaftliche und methodisch Vorgehen reflektiert darzustellen.
- themenbezogene Fragen von Fachexperten (Gutachter der Masterarbeit) aktiv zu beantworten.

Kursinhalt

- Das Kolloquium umfasst eine Präsentation der wichtigsten Ergebnisse der Masterarbeit, gefolgt von der Beantwortung von Fachfragen der Gutachter durch den Studierenden.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Renz, K.-C. (2016): Das 1 x 1 der Präsentation. Für Schule, Studium und Beruf. 2. Auflage, Springer Gabler, Wiesbaden.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Abschlussarbeit
-----------------------------------	-----------------------------------

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	Online Tests: Nein
Prüfungsleistung	Kolloquium

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

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung.