MODULHANDBUCH

Bachelor of Science

Bachelor Cyber Security (FS-BACSD)

180 ECTS

Fernstudium

INTERNATIONALE HOCHSCHULE

Inhaltsverzeichnis

---

3. Semester

---

4. Semester

---

5. Semester

2021-11-01

1. Semester

Betriebssysteme, Rechnernetze und verteilte Systeme

Modulcode: DLBIBRVS

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Paul Libbrecht (Betriebssysteme, Rechnernetze und verteilte Systeme)

Kurse im Modul

- Betriebssysteme, Rechnernetze und verteilte Systeme (DLBIBRVS01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Betriebssysteme
- Rechnernetze
- Verteilte Systeme
- Mobile Computing

Qualifikationsziele des Moduls

Betriebssysteme, Rechnernetze und verteilte Systeme

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Betriebssysteme, Rechnernetze und verteilte Systeme

Kurscode: DLBIBRVS01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch			keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Grundlagen der Betriebssysteme
   - 1.1 Grundlegender Aufbau von Computersystemen
   - 1.2 Dateisysteme
   - 1.3 Speicherverwaltung
   - 1.4 Prozesse und Threads
2. Verbreitete Betriebssysteme
   - 2.1 Grundkonzepte Windows
   - 2.2 Grundkonzepte Unix und Linux
   - 2.3 Grundkonzepte Apple-Betriebssysteme
   - 2.4 Mobile Betriebssysteme

3. Rechnernetze
   - 3.1 Grundlagen der Datenübertragung
   - 3.2 OSI-Referenzmodell
   - 3.3 Netztopologien

4. TCP/IP und Internet
   - 4.1 Entstehung des Internets
   - 4.2 TCP/IP-Protokollstack
   - 4.3 Ausgewählte IP-basierte Protokolle und Dienste
   - 4.4 Sicherheit im Internet

5. Architekturen verteilter Systeme
   - 5.1 Client-Server-Systeme und verteilte Anwendungen
   - 5.2 Grundbegriffe verteilter Systeme: Nebenläufigkeit, Semaphoren, Deadlock
   - 5.3 Kommunikation in verteilten Systemen
   - 5.4 Dienste-Orientierung: SOA, Webservices und Microservices
   - 5.5 Cloud-Anwendungen
   - 5.6 Transaktionen in verteilten Systemen
   - 5.7 High-Performance Computing Cluster

6. Mobile Computing
   - 6.1 Grundlagen, Techniken und Protokolle für Mobile Computing
   - 6.2 Mobiles Internet und seine Anwendungen
   - 6.3 Mobile Kommunikationsnetze
   - 6.4 Sicherheit und Datenschutz in mobilen Systemen

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Einführung in Datenschutz und IT-Sicherheit

Modulcode: DLBINGEDS

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Einführung in Datenschutz und IT-Sicherheit (DLBISIC01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Einführung in Datenschutz und IT-Sicherheit

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Einführung in Datenschutz und IT-Sicherheit

Kurscode: DLBISIC01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

4. Standards und Normen der IT-Sicherheit
   - 4.1 Grundlegende Standards und Normen
   - 4.2 Spezifische Standards und Normen

5. Erstellung eines IT-Sicherheitskonzeptes auf Basis von IT-Grundschutz
   - 5.1 Strukturanalyse
   - 5.2 Schutzbedarfsfeststellung
   - 5.3 Modellierung (Auswahl der Sicherheitsanforderungen)
   - 5.4 IT-Grundschutz-Check
   - 5.5 Risikoanalyse

6. Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte
   - 6.1 Schutz vor Diebstahl
   - 6.2 Schutz vor Schadsoftware (Malware)
   - 6.3 Sichere Anmeldeverfahren
   - 6.4 Sichere Speicherung von Daten
   - 6.5 Sichere Vernichtung von Daten

7. Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen
   - 7.1 Objektschutz
   - 7.2 Schutz vor unerlaubter Datenübertragung
   - 7.3 Schutz vor unerwünschtem Datenverkehr
   - 7.4 Schutz durch Notfallplanung

Literatur

Pflichtliteratur

Weiterführende Literatur

- Harich, T. (2015): IT-Sicherheit im Unternehmen. Mitp, Frechen. 978-3958451285
- Kappes, M. (2013): Netzwerk- und Datensicherheit. Eine praktische Einführung. 2. Auflage, Springer Vieweg, Wiesbaden.
- Kersken, S. (2015): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 7. Auflage, Rheinwerk, Bonn.
- Stumper, K. (2017): Datenschutz – simplified. Persönlichkeitsrechte im Betrieb. epubli, Berlin.
- Willems, E. (2015): Cybergefahr: Wie wir uns gegen Cyber-Crime und Online-Terror wehren können. Springer Vieweg, Wiesbaden.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Mathematik: Analysis

Modulcode: DLBBIMD

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Timo Heinisch (Mathematik: Analysis)

Kurse im Modul

- Mathematik: Analysis (DLBBIMD01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Mathematik: Analysis

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Ist Grundlage für weitere Module im Bereich Bauingenieurwesen	Alle Bachelor-Programme im Bereich Design, Architektur & Bau

Mathematik: Analysis

Kurscode: DLBBIMD01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Differentialrechnung
   - 3.1 Erste Ableitung und Potenzregel
   - 3.2 Ableitungsregeln und höhere Ableitungen
   - 3.3 Taylorreihe und Taylorpolynom
   - 3.4 Kurvendiskussion
   - 3.5 Ausblick: partielle Ableitungen

4. Integralrechnung
   - 4.1 Das unbestimmte Integral und Integrationsregeln
   - 4.2 Das bestimmte Integral und der Hauptsatz der Differential- und Integralrechnung
   - 4.3 Volumen und Mantelfläche von Rotationskörpern sowie Bogenlänge

5. Differentialgleichungen
   - 5.1 Einführung und Grundbegriffe
   - 5.2 Lösung von linearen homogenen Differentialgleichungen erster Ordnung
   - 5.3 Lösung von linearen inhomogenen Differentialgleichungen erster Ordnung
   - 5.4 Ausblick: partielle Differentialgleichungen

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☑ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBBIMD01

Einführung in das wissenschaftliche Arbeiten

Modulcode: DLBWIR-01

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Maya Stagge (Einführung in das wissenschaftliche Arbeiten)

Kurse im Modul

- Einführung in das wissenschaftliche Arbeiten (BWIR01-01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Kombistudium Workbook (best. / nicht bestanden) Studienformat: Fernstudium Workbook (best. / nicht bestanden)	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Wissenschaftstheoretische Grundlagen und Forschungsparadigmen
- Anwendung guter wissenschaftlicher Praxis
- Methodenlehre
- Bibliothekswesen: Struktur, Nutzung und Literaturverwaltung
- Formen wissenschaftlichen Arbeitens an der IUBH

Qualifikationsziele des Moduls

Einführung in das wissenschaftliche Arbeiten

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- formale Kriterien einer wissenschaftlichen Arbeit zu verstehen und anzuwenden.
- grundlegende Forschungsmethoden zu unterscheiden und Kriterien guter wissenschaftlicher Praxis zu benennen.
- zentrale wissenschaftstheoretische Grundlagen und Forschungsparadigmen sowie deren Auswirkungen auf wissenschaftliche Forschungsergebnisse zu beschreiben.
- Literaturdatenbanken, Literaturverwaltungsprogramme sowie weitere Bibliotheksstrukturen sachgerecht zu nutzen, Plagiate zu vermeiden und Zitationsstile korrekt anzuwenden.
- die Evidenzkriterien auf wissenschaftliche Texte anzuwenden.
- ein Forschungsthema einzugrenzen und daraus eine Gliederung für wissenschaftliche Texte abzuleiten.
- ein Literatur-, Abbildungs-, Tabellen- und Abkürzungsverzeichnis für wissenschaftliche Texte zu erstellen.
- die unterschiedlichen Formen des wissenschaftlichen Arbeitens an der IUBH zu verstehen und voneinander zu unterscheiden.

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

Einführung in das wissenschaftliche Arbeiten

Kurscode: BWIR01-01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Die Anwendung guter wissenschaftlicher Praxis gehört zu den akademischen Basisqualifikationen, die im Verlaufe eines Studiums erworben werden sollten. In diesem Kurs geht es um die Unterscheidung zwischen Alltagswissen und Wissenschaft. Dafür ist ein tieferes wissenschaftstheoretisches Verständnis ebenso notwendig, wie das Kennenlernen grundlegender Forschungsmethoden und Instrumente zum Verfassen wissenschaftlicher Texte. Die Studierenden erhalten daher erste Einblicke in die Thematik und werden an Grundlagenwissen herangeführt, dass ihnen zukünftig beim Erstellen wissenschaftlicher Arbeiten hilft. Darüber hinaus erhalten die Studierenden einen Überblick über die unterschiedlichen IUBH Prüfungsformen und einen Einblick in deren Anforderungen und Umsetzung.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- formale Kriterien einer wissenschaftlichen Arbeit zu verstehen und anzuwenden.
- grundlegende Forschungsmethoden zu unterscheiden und Kriterien guter wissenschaftlicher Praxis zu benennen.
- zentrale wissenschaftstheoretische Grundlagen und Forschungsparadigmen sowie deren Auswirkungen auf wissenschaftliche Forschungsergebnisse zu beschreiben.
- Literaturdatenbanken, Literaturverwaltungsprogramme sowie weitere Bibliotheksstrukturen sachgerecht zu nutzen, Plagiate zu vermeiden und Zitationsstile korrekt anzuwenden.
- die Evidenzkriterien auf wissenschaftliche Texte anzuwenden.
- ein Forschungsthema einzugrenzen und daraus eine Gliederung für wissenschaftliche Texte abzuleiten.
- ein Literatur-, Abbildungs-, Tabellen- und Abkürzungsverzeichnis für wissenschaftliche Texte zu erstellen.
- die unterschiedlichen Formen des wissenschaftlichen Arbeitens an der IUBH zu verstehen und voneinander zu unterscheiden.

Kursinhalt

1. Wissenschaftstheorie
   - 1.1 Einführung in Wissenschaft und Forschung
   - 1.2 Forschungsparadigmen
   - 1.3 Grundentscheidungen der Forschung
   - 1.4 Auswirkungen wissenschaftlicher Paradigmen auf das Forschungsdesign

2. Anwendungen guter wissenschaftlier Praxis
   - 2.1 Forschungsethik
   - 2.2 Evidenzlehre
   - 2.3 Datenschutz und eidesstattliche Erklärung
   - 2.4 Orthografie und Form
   - 2.5 Themenfindung und Abgrenzung
   - 2.6 Forschungsfragestellung und Gliederung

3. Forschungsmethoden
   - 3.1 Empirische Forschung
   - 3.2 Literatur- und Übersichtsarbeiten
   - 3.3 Quantitative Datenerhebung
   - 3.4 Qualitative Datenerhebung
   - 3.5 Methodenmix
   - 3.6 Methodenkritik und Selbstreflexion

4. Bibliothekswesen: Struktur, Nutzung und Literaturverwaltung
   - 4.1 Plagiatsprävention
   - 4.2 Datenbankrecherche
   - 4.3 Literaturverwaltung
   - 4.4 Zitation und Autorenrichtlinien
   - 4.5 Literaturverzeichnis

5. Wissenschaftliches Arbeiten an der IUBH – die Hausarbeit / Seminararbeit
6. Wissenschaftliches Arbeiten an der IUBH – der Projektbericht
7. Wissenschaftliches Arbeiten an der IUBH – die Fallstudie
8. Wissenschaftliches Arbeiten an der IUBH – Bachelorarbeit
9. Wissenschaftliches Arbeiten an der IUBH – die Fachpräsentation
10. Wissenschaftliches Arbeiten an der IUBH – die Projektpräsentation
11. Wissenschaftliches Arbeiten an der IUBH – das Kolloquium
12. Wissenschaftliches Arbeiten an der IUBH – das Portfolio
13. Wissenschaftliches Arbeiten an der IUBH – die Klausur

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Bortz, J./Döring, N. (2012): Forschungsmethoden und Evaluation. Für Human- und Sozialwissenschaftler. 5. Auflage, Springer Medizin Verlag, Heidelberg. ▪ Braunecker, C. (2016): How to do Empirie, how to do SPSS – eine Gebrauchsanleitung. Facultas Verlags- und Buchhandels AG, Wien. ▪ Engelen, E.M. et al. (2010): Heureka – Evidenzkriterien in den Wissenschaften, ein Kompendium für den interdisziplinären Gebrauch. Spektrum akademischer Verlag, Heidelberg. ▪ Flick, U. et al. (2012): Handbuch Qualitative Sozialforschung. Grundlagen, Konzepte, Methoden und Anwendungen. 3. Auflage, Beltz Verlag, Weinheim. ▪ Hug, T./Poscheschnik, G. (2015): Empirisch Forschen, 2. Auflage, Verlag Huter & Roth KG, Wien. ▪ Hussy, W. et al. (2013): Forschungsmethoden in Psychologie und Sozialwissenschaften. 2. Auflage, Springer Medizin Verlag, Heidelberg.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Workbook (best. / nicht bestanden)

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☑ Vodcast
- ☐ Shortcast
- ☑ Audio
- ☐ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☑ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Workbook (best. / nicht bestanden)

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☑ Vodcast
- ☐ Shortcast
- ☑ Audio
- ☐ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☑ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Einführung in die Programmierung mit Python

Modulcode: DLBDSIPWP_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Dr.-Ing. Reza Shahbazfar (Einführung in die Programmierung mit Python)

Kurse im Modul

- Einführung in die Programmierung mit Python (DLBDSIPWP01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Einführung in die Programmierung mit Python

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Einführung in die Programmierung mit Python

Kurscode: DLBDSIPWP01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Erklärungen
   - 3.1 Zuweisung, Ausdrücke und Druck
   - 3.2 Bedingte Anweisungen
   - 3.3 Schleifen
   - 3.4 Iteratoren und Verständnisse

4. Funktionen
   - 4.1 Funktionserklärung
   - 4.2 Umfang
   - 4.3 Argumente

5. Fehler und Ausnahmen
   - 5.1 Fehler
   - 5.2 Behandlung von Ausnahmen
   - 5.3 Protokolle

6. Module und Pakete
   - 6.1 Verwendung
   - 6.2 Namensräume
   - 6.3 Dokumentation
   - 6.4 Populäre Datenwissenschaftspakete

Literatur

Pflichtliteratur

Weiterführende Literatur

- Barry, P. (2016): Head first Python. A brain-friendly guide.2nd ed., O'Reilly, Sebastopol, CA.
- Lubanovic, B. (2019): Introducing Python. 2nd ed., O'Reilly, Sebastopol, CA.
- Lutz, M. (2013). Learning Python. 5th ed., O'Reilly, Sebastopol, CA.
- Matthes, E. (2019): Python crash course. A hands-on, project-based introduction to programming. 2nd ed., No Starch Press, San Francisco, CA.
- Ramalho, L. (2015): Fluent Python. Clear, concise, and effective programming. O'Reilly, Sebastopol, CA.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Statistik - Wahrscheinlichkeit und deskriptive Statistik

Modulcode: DLBDSSPDS_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Dr. Stefan Stöckl (Statistik - Wahrscheinlichkeit und deskriptive Statistik)

Kurse im Modul

- Statistik - Wahrscheinlichkeit und deskriptive Statistik (DLBDSSPDS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Statistik - Wahrscheinlichkeit und deskriptive Statistik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Statistik - Wahrscheinlichkeit und deskriptive Statistik

Kurscode: DLBDSSPDS01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Zufallsvariablen
   - 2.1 Zufallsvariablen
   - 2.2 Verteilungsfunktionen und Wahrscheinlichkeitsfunktionen
   - 2.3 Wichtige diskrete Wahrscheinlichkeitsverteilungen
   - 2.4 Wichtige kontinuierliche Wahrscheinlichkeitsverteilungen

3. Gemeinsame Verteilungen
   - 3.1 Gemeinsame Verteilungen
   - 3.2 Randverteilungen
   - 3.3 Unabhängige Zufallsvariablen
   - 3.4 Bedingte Verteilungen

4. Erwartungswert und Varianz
   - 4.1 Erwartungswert einer Zufallsvariablen, bedingter Erwartungswert
   - 4.2 Varianz und Kovarianz
   - 4.3 Erwartungswerte und Varianzen wichtiger Wahrscheinlichkeitsverteilungen
   - 4.4 Algebraische und zentrale Momente
   - 4.5 Momenterzeugende Funktionen

5. Ungleichheiten und Grenzwertsätze
   - 5.1 Wahrscheinlichkeitsungleichheiten
   - 5.2 Ungleichheiten und Erwartungswerte
   - 5.3 Das Gesetz der großen Zahlen
   - 5.4 Zentraler Grenzwertsatz

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Bamberg, G. / Baur, F. / Krapp, M. (2017): Statistik: Eine Einführung für Wirtschafts- und Sozialwissenschaftler, 18. Auflage, De Gruyter Studium. ▪ Bruce, P. / Bruce, A. (2017): Practical statistics for data scientists: 50 essential concepts. O'Reilley, Sebastopol, CA. ▪ Downey, A. B. (2014): Think stats. 2nd edition, O'Reilly, Sebastopol, CA. ▪ Downey, A. B. (2013): Think Bayes. O'Reilly, Sebastopol, CA. ▪ Grabinger, B. (2018): Fit fürs Studium – Statistik, Rheinwerk Verlag. ▪ Quatember, A. (2017): Statistik ohne Angst vor Formeln, 5. Auflage, Pearson Studium. ▪ Reinhart, A. (2015): Statistics done wrong: The woefully complete guide. No Starch Press, San Francisco, CA. ▪ Wassermann, L. (2004): All of statistics: A concise course in statistical inference. Springer Science+Business Media, New York, NY. ▪ Wewel, M. C. / Blatter, A. (2019): Statistik im Bachelor-Studium der BWL und VWL: Methoden, Anwendung, Interpretation, 4. Auflage, Pearson Studium.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☑ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

2. Semester

Grundlagen der objektorientierten Programmierung mit Java

Modulcode: DLBINGOPJ

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Grundlagen der objektorientierten Programmierung mit Java (IOBP01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Grundlagen der objektorientierten Programmierung mit Java

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Grundlagen der objektorientierten Programmierung mit Java

Kurscode: IOBP01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Mathematik: Lineare Algebra

Modulcode: DLBBIM

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Moustafa Nawito (Mathematik: Lineare Algebra)

Kurse im Modul

- Mathematik: Lineare Algebra (DLBBIM01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Mathematik: Lineare Algebra

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Mathematik: Lineare Algebra

Kurscode: DLBBIM01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Grundlagen
   - 1.1 Lineare Gleichungssysteme
   - 1.2 Matrizen als kompakte Repräsentation linearer Gleichungssysteme
   - 1.3 Matrix Algebra
   - 1.4 Inverse und Spur
2. Vektor-Räume
   - 2.1 Definition
   - 2.2 Linear-Kombination und lineare Abhängigkeit
   - 2.3 Basis, lineare Hülle und Rang

3. Lineare und affine Abbildungen
   - 3.1 Matrix-Repräsentation linearer Abbildungen
   - 3.2 Bild und Kern
   - 3.3 Affine Räume und Unter-Räume
   - 3.4 Affine Abbildungen

4. Analytische Geometrie
   - 4.1 Norm
   - 4.2 Skalar- und Vektorprodukt
   - 4.3 Orthogonale Projektionen
   - 4.4 Rotationen

5. Matrix Zerlegung
   - 5.1 Determinante und Spur
   - 5.2 Eigenwerte and Eigenvektoren
   - 5.3 Cholesky-Zerlegung
   - 5.4 Eigenwertzerlegung und Diagonalisierung
   - 5.5 Singulärwertzerlegung

Literatur

Pflichtliteratur

Weiterführende Literatur

- Arens, T. et al. (2013): Grundwissen Mathematikstudium. Analysis und Lineare Algebra mit Querverbindungen. Springer Berlin/Heidelberg.
- Boas, Mary L. (2006): Mathematical methods in the physical sciences. Third edition. Wiley, Hoboken/NJ.
- Deisenroth, M. P./Faisal, A./Ong C.-S. (2018): Math for ML. Cambridge University Press. (URL: https://mml-book.com [letzter Zugriff: 04.03.2019]).
- Fischer, G. (2017): Lernbuch Lineare Algebra und Analytische Geometrie. Springer Spektrum (Lehrbuch), Wiesbaden.
- Modler, F./Kreh, M. (2014): Tutorium Analysis 1 und Lineare Algebra 1. Mathematik von Studenten für Studenten erklärt und kommentiert. 3. Auflage, Springer, Berlin/Heidelberg.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☑ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☑ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Kollaboratives Arbeiten

Modulcode: DLBKA

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Karin Halbritter (Kollaboratives Arbeiten)

Kurse im Modul

- Kollaboratives Arbeiten (DLBKA01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Fachpräsentation Studienformat: Kombistudium Fachpräsentation	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Kollaboratives Arbeiten

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Das Modul ist eigenständig. Es liefert Grundlagenkenntnisse für alle weiteren Module.	Alle Bachelor-Studiengänge des IUBH-Fernstudiums

Kollaboratives Arbeiten

Kurscode: DLBKA01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Networking & Kooperation
   - 2.1 Die passenden Kooperationspartner finden und gewinnen
   - 2.2 Tragfähige Beziehungen: Digital Interaction und Vertrauensaufbau
   - 2.3 Zusammenarbeit – lokal und virtuell organisieren & Medien einsetzen
   - 2.4 Social Learning: Lernprozesse agil, kollaborativ und mobil planen

3. Performance in (virtuellen) Teams
   - 3.1 Ziele, Rollen, Organisation und Performance Measurement
   - 3.2 Team Building und Team Flow
   - 3.3 Scrum als Rahmen für agiles Projektmanagement
   - 3.4 Design Thinking, Kanban, Planning Poker, Working-in-Progress-Limits & Co

4. Kommunizieren und überzeugen
   - 4.1 Kommunikation als soziale Interaktion
   - 4.2 Sprache, Bilder, Metaphern und Geschichten
   - 4.3 Die Haltung macht's: offen, empathisch und wertschätzend kommunizieren
   - 4.4 Aktiv zuhören – argumentieren – überzeugen – motivieren
   - 4.5 Die eigene Gesprächs- und Argumentationsführung analysieren

5. Konfliktpotenziale erkennen –Konflikte handhaben –wirksam verhandeln
   - 5.1 Vielfalt respektieren – Chancen nutzen
   - 5.2 Empathie für sich und andere entwickeln
   - 5.3 Systemische Lösungsarbeit und Reframing
   - 5.4 Konstruktiv verhandeln: klare Worte finden – Interessen statt Positionen

6. Eigene Projekte realisieren
   - 6.1 Wirksam Ziele setzen – fokussieren – reflektieren
   - 6.2 Vom agilen Umgang mit der eigenen Zeit
   - 6.3 (Selbst-)Coaching und Inneres Team
   - 6.4 Strategien und Methoden der Selbstführung und -motivation

7. Eigene Ressourcen mobilisieren
   - 7.1 Ressourcen erkennen – Emotionen regulieren
   - 7.2 Reflexion und Innovation – laterales Denken und Kreativität
   - 7.3 Transferstärke und Willenskraft: Bedingungsfaktoren analysieren und steuern

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Fachpräsentation

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Fachpräsentation

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

Einführung in die Netzwerkforensik

Modulcode: DLBCSEINF_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Alexander Lawall (Einführung in die Netzwerkforensik)

Kurse im Modul

- Einführung in die Netzwerkforensik (DLBCSEINF01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Einführung in die Netzwerkforensik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Einführung in die Netzwerkforensik

Kurscode: DLBCSEINF01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBIBRVS01 oder DLBIBRVS01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Warum Netzwerk-Forensik?
   - 1.1 Ziele der Untersuchungen
   - 1.2 Beweiserhebung im Netzwerk
   - 1.3 Erkennung von Eindringlingen
   - 1.4 (D)Dos-Erkennung und Entschärfung
   - 1.5 Marktverfügbare Werkzeuge

2. Grundlegende Protokoll-Schichtung
   - 2.1 Internet-Protokoll-Hierarchie
   - 2.2 Verbindung und verbindungslose Protokolle
   - 2.3 Lesen von RFCs und zugehöriger Dokumentation

3. TCP vs. UDP
   - 3.1 Verbindungsloses UDP
   - 3.2 TCP-Verbindungsaufbau
   - 3.3 Fehlende Pakete und Weiterleitung
   - 3.4 SOCKS-Proxying
   - 3.5 Angriffe gegen TCP und UDP

4. Das Internet-Protokoll
   - 4.1 IP-Adressen, IPv4 und IPv6
   - 4.2 Erlangen einer IPv4- und IPv6-Adresse
   - 4.3 Die Rolle der ICANN
   - 4.4 IP-Firewalls und Übersetzung von IP-Netzwerkadressen
   - 4.5 SOCKS-Proxying

5. Routing des Link-Layers
   - 5.1 ARP (Adressauflösungsprotokoll)
   - 5.2 Dynamisches RIP-Routing
   - 5.3 BGP-Peering
   - 5.4 Autonome Systemnummern
   - 5.5 Angriffe gegen Routing

6. Domänennamen-System
   - 6.1 Hostnamen-Hierarchie
   - 6.2 DNS als verteilte Datenbank
   - 6.3 DNSSEC
   - 6.4 SPF, DMARC und andere Sonderaufzeichnungen

7. Gemeinsame Protokolle der Anwendungs-Schicht
   - 7.1 HTTP
   - 7.2 HTTP/2
   - 7.3 SMTP

8. Transportschicht-Verschlüsselung
   - 8.1 SSH
   - 8.2 IPSEC
   - 8.3 TLS
   - 8.4 Man-In-The-Middle-Attack
   - 8.5 Zertifikate und Zertifizierungsstellen

9. Systeme zur Erkennung und Verhinderung von Eindringung
   - 9.1 Sensor- und Ereignistypen
   - 9.2 Netflow-Überwachung
   - 9.3 Regeln, falsch positive und falsch negative Ergebnisse
   - 9.4 SIEMs
   - 9.5 Technologien zur Angriffsvorbeugung

10. Korrelations- und Anreicherungsdatenquellen
    - 10.1 Anreicherung von Daten
    - 10.2 DNS-Datenquellen: DNSBLs, passives DNS, DNS-Repositorien
    - 10.3 AS-Nummern, IP-Blöcke, GeoIP- und WhoIs-Daten
    - 10.4 Zertifikat-Transparenz
    - 10.5 Korrelationsmethoden

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBCSEINF01_D

Requirements Engineering

Modulcode: IREN

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Tobias Brückmann (Requirements Engineering)

Kurse im Modul

- Requirements Engineering (IREN01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Requirements Engineering

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Requirements Engineering

Kurscode: IREN01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Ausgewählte Ermittlungstechniken
   - 3.1 Kreativitätstechniken
   - 3.2 Befragungstechniken
   - 3.3 Beobachtungstechniken
   - 3.4 Prototyping

4. Dokumentation von Anforderungen
   - 4.1 Aktivitäten zur Dokumentation von Anforderungen
   - 4.2 Typische Elemente der Anforderungsdokumentation
   - 4.3 Dokumentationsformen

5. Modellierung von Prozessen
   - 5.1 Grundlagen und Begriffe
   - 5.2 Modellierung mit der Business Process Model and Notation
   - 5.3 Modellierung mit Ereignisgesteuerten Prozessketten

6. Modellierung von Systemen
   - 6.1 Grundlagen Unified Modeling Language
   - 6.2 UML-Use Case-Diagramm
   - 6.3 UML-Aktivitätsdiagramm
   - 6.4 UML-Klassendiagramm
   - 6.5 UML-Zustandsdiagramm

7. Prüfen und Abstimmen von Anforderungen
   - 7.1 Aktivitäten zum Prüfen und Abstimmen von Anforderungen
   - 7.2 Prüfkriterien
   - 7.3 Prüfprinzipien
   - 7.4 Prüftechniken
   - 7.5 Abstimmen von Anforderungen

8. Management von Anforderungen und Techniken zur Priorisierung
   - 8.1 Verwalten von Anforderungen
   - 8.2 Techniken zur Priorisierung von Anforderungen

Literatur

Pflichtliteratur

Weiterführende Literatur

- Allweyer T. (2009): BPMN 2.0. Business Process Model and Notation. 2. Auflage, Books on Demand, Norderstedt.
- Balzert, H. (2010): UML 2 kompakt. 3. Auflage, Springer Spektrum, Wiesbaden.
- Booch, G./Rumbaugh, J./Jacobson, I. (2006): Das UML-Benutzerhandbuch. Addison-Wesley, Boston.
- Cohn, M. (2010): User Stories. Für die agile Software-Entwicklung mit Scrum, XP u.a. mitp, Wachtendonk.
- Freund, J./Rücker, B. (2012): Praxishandbuch BPMN 2.0. 3. Auflage, Carl Hanser Verlag, München.
- Gadatsch A. (2013): Grundkurs Geschäftsprozess-Management. 7. Auflage, Vieweg+Teubner, Wiesbaden.
- Pohl, K. (2008): Requirements Engineering. Grundlagen, Prinzipien, Techniken. 2. Auflage, dpunkt.verlag, Heidelberg.
- Pohl, K./Rupp, C. (2011): Basiswissen Requirements Engineering. 3. Auflage, dpunkt.verlag, Heidelberg.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Grundzüge des System-Pentestings

Modulcode: DLBCSESPB_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Jesus Luna Garcia (Grundzüge des System-Pentestings)

Kurse im Modul

- Grundzüge des System-Pentestings (DLBCSESPB01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Grundzüge des System-Pentestings

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Grundzüge des System-Pentestings

Kurscode: DLBCSESPB01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Hintergrundkonzepte
   - 2.1 Betriebssysteme
   - 2.2 Hardware-Architekturen
   - 2.3 Netzwerke und Protokolle
   - 2.4 Web-basierte Anwendungen
   - 2.5 Cloud-Computing

3. Ablauf von Penetrationstests
   - 3.1 Planung und Erkundung
   - 3.2 Whitebox-, Blackbox- und Graybox-Scanning
   - 3.3 Zugang erhalten
   - 3.4 Aufrechterhaltung des Zugangs
   - 3.5 Analyse und Berichterstattung
   - 3.6 Härtung und Entschärfung

4. Betriebssystembasierte Penetrationstests
   - 4.1 Häufige Fehlkonfigurationen
   - 4.2 Shellcode-Angriffe
   - 4.3 Speicherkorruption und Pufferüberlauf-Schwachstellen
   - 4.4 Metasploit und Kali-Tools
   - 4.5 Härtung des Betriebssystems

5. Netzwerk-Penetrationstests
   - 5.1 Scoping und Recon der Netzwerkinfrastruktur
   - 5.2 Ausnutzen von Netzwerkdiensten
   - 5.3 Seitliche Bewegung im Netzwerk
   - 5.4 Kerberos-Angriffe
   - 5.5 Werkzeugsatz: Nmap, PowerShell, Bloodhound und Tcpdump
   - 5.6 Entwickeln von Korrekturmaßnahmen

6. Web-App-Penetrationstests
   - 6.1 Die OWASP-Methodik
   - 6.2 Open-Source-Intelligenz (OSINT)
   - 6.3 Häufig ausgenutzte Web-App-Schwachstellen
   - 6.4 Ausnutzungs-Toolset: BurpSuite, sqlmap, BeEF und ExploitDB
   - 6.5 Berichterstattung über Ergebnisse und Abhilfemaßnahmen

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

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bundesamt für Sicherheit in der Informationstechnologie (2016): Praxis-Leitfaden. IT-Sicherheits-Penetrationstest. (URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html [letzter Zugriff: 11.3.2021]).
- Bundesamt für Sicherheit in der Informationstechnologie (2020): Studie zur Durchführung von Penetrationstests. (URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3 [letzter Zugriff: 11.3.2021]).
- Faircloth, J. (2017): Pentesting mit Open Source. Professionelle Penetrationstests mit kostenloser und quelloffener Software. Franzis Verlag, München.
- Gollmann, D. (2011): Computer Security. 3rd edition, Wiley, Hoboken, NJ.
- Lin, X. (2018): Introductory Computer Forensics. A Hands-on Practical Approach. Springer International Publishing, Cham.
- Yurichev, D. (2020): Reverse Engineering for Beginners. (URL: https://beginners.re/ [Retrieved: 24.08.2020]).

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

3. Semester

Interkulturelle und ethische Handlungskompetenzen

Modulcode: DLBIHK

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Interkulturelle und ethische Handlungskompetenzen (DLBIHK01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Interkulturelle und ethische Handlungskompetenzen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Das Modul ist eigenständig. Es liefert Grundlagenkenntnisse für alle weiteren Module.	Alle Bachelor-Studiengänge des IUBH-Fernstudiums

Interkulturelle und ethische Handlungskompetenzen

Kurscode: DLBIHK01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Kulturkonzepte
   - 2.1 Hofstedes Kulturdimensionen
   - 2.2 Kulturdifferenzierung nach Hall
   - 2.3 Locus-of-Control-Konzept nach Rotter

3. Kultur und Ethik
   - 3.1 Ethik – Grundbegriffe und Konzepte
   - 3.2 Interdependenz von Kultur und Ethik
   - 3.3 Ethische Konzepte in verschiedenen Regionen der Welt

4. Aktuelle Themen im Bereich Interkulturalität, Ethik und Diversity
   - 4.1 Digital Ethics
   - 4.2 Gleichberechtigung und Gleichstellung
   - 4.3 Social Diversity

5. Interkulturelles Lernen und Arbeiten
   - 5.1 Akkulturation
   - 5.2 Lernen und Arbeiten in interkulturellen Arbeitsgruppen
   - 5.3 Strategien zum Umgang mit kulturell geprägten Konflikten

6. Fallbeispiele für kulturelle und ethische Konflikte
   - 6.1 Fallbeispiel Interkulturalität
   - 6.2 Fallbeispiel Diversity
   - 6.3 Fallbeispiel Interkulturalität und Ethik

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Fallstudie

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Fallstudie

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

DLBIHK01

Einführung in das Internet of Things

Modulcode: DLBINGEIT

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Einführung in das Internet of Things (DLBINGEIT01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Einführung in das Internet of Things

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Einführung in das Internet of Things

Kurscode: DLBINGEIT01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Kommunikationsstandards und -technologien
   - 3.1 Netzwerktopologien
   - 3.2 Netzwerkprotokolle
   - 3.3 Technologien

4. Datenspeicherung und -verarbeitung
   - 4.1 Vernetztes Speichern mit Linked Data und RDF(S)
   - 4.2 Analyse vernetzer Daten mit dem Semantic Reasoner
   - 4.3 Verarbeitung von Datenströmen mit Complex Event Processing
   - 4.4 Betrieb und Analyse großer Datenmengen mit NoSQL und MapReduce

5. Design und Entwicklung
   - 5.1 Software Engineering für verteilte und eingebettete Systeme
   - 5.2 Architekturstile und -muster verteilter Systeme
   - 5.3 Plattformen: Mikrocontroller, Einplatinenrechner, Ein-Chip-Systeme

6. Anwendungsbereiche
   - 6.1 Smarthome/Smart Living
   - 6.2 Ambient Assisted Living
   - 6.3 Smart Energy/Smart Grid
   - 6.4 Smart Factory
   - 6.5 Smart Logistics

Literatur

Pflichtliteratur

Weiterführende Literatur

- Andelfinger, V. P./Hänisch, T. (Hrsg.) (2015): Internet der Dinge. Technik, Trends und Geschäftsmodelle. Springer, Wiesbaden.
- Buyya, R./Vahid Dastjerdi, A. (Hrsg.) (2016): Internet of things. Principles and paradigms. Morgan Kaufmann, Cambridge (MA).
- Christoph, E./Sprenger, F. (Hrsg.) (2015): Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt. transcript, Bielefeld.
- Fleisch, E. (Hrsg.) (2005): Internet der dinge. Ubiquitous Computing und RFID in der Praxis. Springer, Berlin.
- Gilchrist, A. (2016): Industry 4.0. The industrial internet of things. Apress, New York.
- Kaufmann, T. (2015): Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge. Der Weg vom Anspruch in die Wirklichkeit. Springer, Wiesbaden.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☑ Vodcast
- ☐ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☑ Vodcast
- ☐ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Algorithmen, Datenstrukturen und Programmiersprachen

Modulcode: DLBIADPS

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	IOBP01, IOBP02	BA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Paul Libbrecht (Algorithmen, Datenstrukturen und Programmiersprachen)

Kurse im Modul

- Algorithmen, Datenstrukturen und Programmiersprachen (DLBIADPS01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Datenstrukturen
- Algorithmen-Entwurf
- Wichtige Algorithmen
- Grundbegriffe XML
- Programmierparadigmen und Grundbegriffe von Programmiersprachen
- Überblick über verbreitete Programmiersprachen

Qualifikationsziele des Moduls

Algorithmen, Datenstrukturen und Programmiersprachen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Algorithmen, Datenstrukturen und Programmiersprachen

Kurscode: DLBIADPS01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IOBP01, IOBP02

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Datenstrukturen
   - 2.1 Weiterführende Datenstrukturen
   - 2.2 Blockchain
   - 2.3 Abstrakte Datentypen, Objekte und Klassen

3. Algorithmenentwurf
   - 3.1 Induktion, Iteration und Rekursion
   - 3.2 Methoden des Algorithmen-Entwurfs
   - 3.3 Korrektheit und Verifikation von Algorithmen
   - 3.4 Effizienz und Komplexität von Algorithmen

4. Grundlegende Algorithmen
   - 4.1 Traversieren und Linearisieren von Bäumen
   - 4.2 Sortieralgorithmen
   - 4.3 Suche in Zeichenketten
   - 4.4 Hash-Algorithmen
   - 4.5 Mustererkennung

5. XML
   - 5.1 Aufbau von XML-Dokumenten
   - 5.2 Zugriff auf XML-Dokumente mit DOM und SAX
   - 5.3 Transformation von XML-Dokumenten mittels XSL
   - 5.4 JSON als Alternative zu XML

6. Programmiersprachen
   - 6.1 Programmierparadigmen
   - 6.2 Ausführung von Programmen
   - 6.3 Typen von Programmiersprachen
   - 6.4 Syntax, Semantik und Pragmatik
   - 6.5 Variablen und Typsysteme

7. Überblick über wichtige Programmiersprachen
   - 7.1 Die C-Familie
   - 7.2 Java
   - 7.3 Matlab
   - 7.4 COBOL
   - 7.5 PHP und HTML
   - 7.6 Weitere Programmiersprachen

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBIADPS01

Theoretische Informatik und Mathematische Logik

Modulcode: DLBITIML

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	DLBIADPS01	BA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Ralf Kneuper (Theoretische Informatik und Mathematische Logik)

Kurse im Modul

- Theoretische Informatik und Mathematische Logik (DLBITIML01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Theoretische Informatik und Mathematische Logik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Theoretische Informatik und Mathematische Logik

Kurscode: DLBITIML01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBIADPS01

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Prädikatenlogik
   - 2.1 Grundbegriffe
   - 2.2 Resolution in der Prädikatenlogik
   - 2.3 Vollständigkeit und Unvollständigkeit
   - 2.4 Logik-Programmierung mit Prolog

3. Endliche Automaten und reguläre Ausdrücke
   - 3.1 Grundbegriffe endlicher Automaten
   - 3.2 Reguläre Ausdrücke und Sprachen
   - 3.3 Praxisanwendungen

4. Formale Sprachen und Grammatiken
   - 4.1 Grundbegriffe
   - 4.2 Die Chomsky-Hierarchie
   - 4.3 Kontextfreie Grammatiken (Typ-2-Grammatiken)
   - 4.4 Kontextsensitive Grammatiken (Typ-1-Grammatiken)

5. Berechenbarkeit und Turing-Maschinen
   - 5.1 Modelle der Berechenbarkeit
   - 5.2 Turing-Maschinen
   - 5.3 Einige weitere Berechnungsmodelle
   - 5.4 Berechenbarkeit, Entscheidbarkeit und das Halteproblem

6. Komplexitätstheorie
   - 6.1 Landau'sche O-Notation
   - 6.2 Grundbegriffe der Komplexitätstheorie
   - 6.3 P=NP?
   - 6.4 NP-vollständige Probleme

7. Petri-Netze
   - 7.1 Grundbegriffe von Graphen und Petri-Netzen
   - 7.2 Modellierung von Eigenschaften nebenläufiger Systeme
   - 7.3 Erreichbarkeit in Petri-Netzen
   - 7.4 Invarianten von Petri-Netzen

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBITIML01

IT-Projektmanagement

Modulcode: IPMG

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Tobias Brückmann (IT-Projektmanagement)

Kurse im Modul

- IT-Projektmanagement (IPMG01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

IT-Projektmanagement

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundprinzipien und Aufgaben von IT-Projektmanagement zu erläutern und voneinander abzugrenzen.
- wichtige, praktische Techniken und Methoden, die für die Durchführung von IT-Projektmanagement erforderlich sind zu beschreiben.
- die grundlegenden Vorgehensmodelle wiederzugeben und deren Vor- und Nachteile sowie deren Einsatzmöglichkeiten zu erläutern.
- auf Basis von gegebenen Praxisszenarien mögliche Projektrisiken zu identifizieren und geeignete Maßnahmen aus dem IT-Projektmanagement zu wählen, um die Risiken gezielt zu minimieren.

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

IT-Projektmanagement

Kurscode: IPMG01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Grundprinzipien und Aufgaben von IT-Projektmanagement zu erläutern und voneinander abzugrenzen.
- wichtige, praktische Techniken und Methoden, die für die Durchführung von IT-Projektmanagement erforderlich sind zu beschreiben.
- die grundlegenden Vorgehensmodelle wiederzugeben und deren Vor- und Nachteile sowie deren Einsatzmöglichkeiten zu erläutern.
- auf Basis von gegebenen Praxisszenarien mögliche Projektrisiken zu identifizieren und geeignete Maßnahmen aus dem IT-Projektmanagement zu wählen, um die Risiken gezielt zu minimieren.

Kursinhalt

1. Begriffe und Grundlagen im IT-Projektmanagement
   - 1.1 Projektbegriff und Arten von IT-Projekten
   - 1.2 IT-Projektlebenszyklus
   - 1.3 Multiprojektmanagement – Das Projekt im Kontext der Organisation
2. Planungstechniken
   - 2.1 Planung im Großen: Meilensteine, Teilaufgaben, Arbeitspakete
   - 2.2 Planung im Großen: Gantt-Diagramme
   - 2.3 Planung und Organisation von Arbeitspaketen: Kanban Board
3. Priorisierung, Aufwandschätzung, Projektcontrolling
   - 3.1 Priorisierung
   - 3.2 Aufwandsschätzung
   - 3.3 Projektcontrolling

4. Stakeholder-, Kommunikations- und Risikomanagement
   - 4.1 Stakeholder Management
   - 4.2 Kommunikationsmanagement
   - 4.3 Risikomanagement

5. Organisation und Struktur im IT-Projektmanagement
   - 5.1 Überblick und Managementebenen von PRINCE2
   - 5.2 Managementprozesse in PRINCE2
   - 5.3 Pragmatisches IT-Projektmanagement (PITPM)
   - 5.4 Konfiguration des IT-Projektes in PITPM
   - 5.5 Steuern des Projekts in PITPM

6. Denkmodelle im IT-Projektmanagement
   - 6.1 Agile Softwareentwicklung
   - 6.2 Value-Based Software Engineering

Literatur

Pflichtliteratur

Weiterführende Literatur

- Berkun, S. (2009): Die Kunst des IT-Projektmanagements. 2. Auflage, O'Reilly, Sebastopol (CA).
- DeMarco, T. (2003): Bärentango. Mit Risikomanagement Projekte zum Erfolg führen. Carl Hanser Verlag, München.
- Geirhos, M. (2011): IT-Projektmanagement. Was wirklich funktioniert – und was nicht. Galileo Computing, Bonn.
- Höhn, R./Höppner S. (2008): Das V-Modell XT. Grundlagen, Methodik und Anwendungen. Springer, Berlin/Heidelberg.
- Malik, M. (2006): Führen, Leisten, Leben. Wirksames Management für eine neue Zeit. Campus, Frankfurt a. M.
- Mangold, P. (2009): IT-Projektmanagement kompakt. 3.Auflage, Spektrum.
- Motzel, E./Pannenbäcker, O. (1998): Projektmanagement-Kanon. Der deutsche Zugang zum Project Management Body of Knowledge. TÜV-Verlag, Köln.
- Patzak, G./Rattay, G.: Projektmanagement. Leitfaden zum Management von Projekten, Projektportfolios und projektorientierten Unternehmen. 5. Auflage, Linde Verlag, Wien.
- Phillips, J. (2010): IT Project Management. On Track from Start to Finish. 3. Auflage, McGraw-Hill, New York.
- Pichler, R. (2007): Scrum. Agiles Projektmanagement erfolgreich einsetzen. dpunkt.verlag, Heidelberg.
- Schwalbe, K. (2010): Information Technology Project Management. 6. Auflage, Course Technology, Independence (KY).
- Tiemeyer, E. (2010): Handbuch IT-Projektmanagement. Vorgehensmodelle, Managementinstrumente, Good Practices. Hanser, München.
- Versteegen, G. (2000): Projektmanagement: mit dem Rational Unified Process. Springer, Berlin/Heidelberg.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DevSecOps und gängige Software-Schwachstellen

Modulcode: DLBCSEDCSW_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (DevSecOps und gängige Software-Schwachstellen)

Kurse im Modul

- DevSecOps und gängige Software-Schwachstellen (DLBCSEDCSW01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Schriftliche Ausarbeitung: Hausarbeit	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

DevSecOps und gängige Software-Schwachstellen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

DevSecOps und gängige Software-Schwachstellen

Kurscode: DLBCSEDCSW01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSESPB01_D oder DLBCSESPB01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Einführung in den Software-Entwicklungsprozess
   - 1.1 Traditionelle Software-Entwicklung: Wasserfall-Methodik
   - 1.2 Iterativer Entwurf
   - 1.3 Agile Software-Entwicklung
   - 1.4 Operationen als separater Prozess
   - 1.5 Infrastruktur als Code
   - 1.6 Zusammenlegung von Entwicklung und Betrieb: DevOps

2. Bewährte Praktiken von DevOps
   - 2.1 Codierung: Code-Entwicklung und -Überprüfung, Quellcode-Verwaltungstools, Code-Zusammenführung.
   - 2.2 Build: kontinuierliche Integrationswerkzeuge, Build-Status.
   - 2.3 Tests: Instrumente für kontinuierliche Tests, die ein schnelles und zeitnahes Feedback zu Geschäftsrisiken liefern.
   - 2.4 Paketierung: Artefakt-Repository, Staging vor der Bereitstellung der Anwendung.
   - 2.5 Freigabe: Änderungsmanagement, Freigabegenehmigungen, Freigabeautomatisierung.
   - 2.6 Konfigurieren: Konfiguration und Verwaltung der Infrastruktur, Infrastruktur als Code-Tools.
   - 2.7 Überwachung: Überwachung der Anwendungsleistung, Endbenutzer-Erfahrung.

3. Quellen von Sicherheitsfehlern
   - 3.1 Allgemeine Klassen von Fehlern
   - 3.2 Ein Blick auf die OWASP-Top Ten
   - 3.3 Blick auf die Mitra CWE™

4. DevSecOps
   - 4.1 Schutzziele
   - 4.2 Modellierung von Bedrohungen
   - 4.3 Wahl der Programmiersprache, Werkzeugkette und Infrastruktur
   - 4.4 Linting bei Fragen der Codesicherheit
   - 4.5 Prüfung auf Sicherheit
   - 4.6 Sicherheit durch Design/Shifting Left
   - 4.7 Der Mensch als ein Problem der Sicherheit
   - 4.8 Entwerfen in einem Fehlerbericht- und Antwortprozess
   - 4.9 Steuern eines Bug-Bounty-Programms

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Hausarbeit

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

4. Semester

IT-Servicemanagement

Modulcode: IWSM1

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. André Köhler (IT-Servicemanagement)

Kurse im Modul

- IT-Servicemanagement (IWSM01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Grundlagen und Begriffe zum IT-Servicemanagement
- IT Infrastructure Library (ITIL)
- ITIL – Service Design
- ITIL – Service Transition
- ITIL – Service Operation
- Information Security Management mit dem IT-Grundschutz-Framework des BSI

Qualifikationsziele des Moduls

IT-Servicemanagement

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

IT-Servicemanagement

Kurscode: IWSM01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Grundlagen und Begriffe zum IT-Service Management
   - 1.1 IT-Dienstleistungen (auch: IT-Services, engl. IT services)
   - 1.2 IT-Servicemanagement
2. IT Infrastructure Library (ITIL)
   - 2.1 Service Livecycle 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 Eventmanagement
   - 5.2 Incident Management
   - 5.3 Problemmanagement
   - 5.4 Weitere Prozesse in der Service Operation

6. Information Security Management mit dem IT-Grundschutz Framework des BSI
   - 6.1 Aufbau und Elemente des BSI-Grundschutzes
   - 6.2 Informationssicherheitsprozess

Literatur

Pflichtliteratur

Weiterführende Literatur

- Beims, M. (2012): IT-Service Management in der Praxis mit ITIL. Hanser, München.
- Bundesamt für Sicherheit und Informationstechnik (Hrsg.) (2008): BSI-Standard 100-1. Managementsysteme für Informationssicherheit (ISMS). (URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile [letzter Zugriff: 27.02.2017]).
- Bundesamt für Sicherheit und Informationstechnik (Hrsg.) (2008): BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise. (URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile [letzter Zugriff: 27.02.2017]).
- Bundesamt für Sicherheit und Informationstechnik (Hrsg.) (2014): IT-Grundschutz-Kataloge. 14. Ergänzungslieferung. (URL: https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2014_EL14_DE.pdf [letzter Zugriff: 27.02.2017]).
- Renner, B./Moser, U./Schmid, D. (2006): IT-Service-Management. Transparente IT-Leistungen & Messbare Qualität. BPX Edition, Rheinfelden.
- Tiemeyer, E. (Hrsg.) (2011): Handbuch IT-Management. Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. Hanser, München.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Kryptografische Verfahren

Modulcode: DLBISIC2

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Ralf Kneuper (Kryptografische Verfahren)

Kurse im Modul

- Kryptografische Verfahren (DLBISIC02)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Kryptografische Verfahren

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Kryptografische Verfahren

Kurscode: DLBISIC02

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Kryptografische Grundanwendungen
   - 3.1 Schlüsselaustausch und hybriden Verfahren
   - 3.2 Digitale Unterschrift
   - 3.3 Message Authentication Code
   - 3.4 Steganografische Verfahren

4. Authentifikation
   - 4.1 Passwörter und Public-Key-Zertifikate
   - 4.2 Challenge-Response-Verfahren und Zero-Knowledge-Verfahren
   - 4.3 Biometrische Verfahren
   - 4.4 Authentifikation in verteilten Systemen
   - 4.5 Identitäten durch Smartcards

5. Sicherung von Einzelrechnern
   - 5.1 Schadsoftware und Cookies
   - 5.2 Einige Besonderheiten bei Betriebssystemen
   - 5.3 Sicherheit von Webservern

6. Sicherheit in Kommunikationsnetzen
   - 6.1 Sicherheitsprobleme und Abwehrkonzepte
   - 6.2 Internet-Standards für die Kommunikationssicherheit
   - 6.3 Identität und Anonymität
   - 6.4 Sicherheit in der mobilen und der drahtlosen Kommunikation

7. Sicherheit im E-Commerce
   - 7.1 E-Mail-Sicherheit
   - 7.2 Online-Banking und Onlinebezahlen
   - 7.3 Elektronisches Geld

8. Sichere Softwareentwicklung
   - 8.1 Bedrohungsmodellierung
   - 8.2 Sicherer Softwareentwurf
   - 8.3 Techniken für sicheres Programmieren

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☐ Live Tutorium/Course Feed

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBISIC02

IT-Recht

Modulcode: DLBIITR

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Sven Jacobs (IT-Recht)

Kurse im Modul

- IT-Recht (DLBIITR01)

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

IT-Recht

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

IT-Recht

Kurscode: DLBIITR01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Typische Vertragstypen in der IT
   - 2.1 Hardware-Verträge
   - 2.2 Softwareüberlassung
   - 2.3 Projektverträge
   - 2.4 Besonderheiten bei agiler Vorgehensweise
   - 2.5 Beratungs- und Wartungsverträge
   - 2.6 Cloud Computing, Outsourcing und Hosting
   - 2.7 Besonderheiten bei der öffentlichen Vergabe von IT-Leistungen
   - 2.8 Kartellrecht

3. Softwarelizenzmodelle
   - 3.1 Lizenzen und Softwareüberlassung
   - 3.2 Standardklauseln
   - 3.3 Durchsetzung von Lizenzen durch Digital Rights Management (DRM)
   - 3.4 Open Source Software, Free- und Shareware

4. Schutz- und Informationsrechte
   - 4.1 Patent- und Markenrecht
   - 4.2 Urheberrecht
   - 4.3 Schutzfähigkeit von Software
   - 4.4 Abmahnungen
   - 4.5 Informationsfreiheitsgesetz

5. Internet- und Telekommunikationsrecht
   - 5.1 Telekommunikationsgesetz
   - 5.2 Telemediengesetz
   - 5.3 Verantwortung für Inhalte im Internet
   - 5.4 Domainrecht
   - 5.5 Elektronische Signaturen
   - 5.6 Elektronische Vertragsschließung
   - 5.7 Elektronischer Geschäftsverkehr und Onlineshopping

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☐ Live Tutorium/Course Feed

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☐ Live Tutorium/Course Feed

Host- und Softwareforensik

Modulcode: DLBCSEHSF_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Host- und Softwareforensik)

Kurse im Modul

- Host- und Softwareforensik (DLBCSEHSF01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Host- und Softwareforensik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Host- und Softwareforensik

Kurscode: DLBCSEHSF01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSESPB01_D oder DLBCSESPB01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Digitale Beweise
   - 2.1 Arten von Beweisen
   - 2.2 Überlegungen zur Erhebung und zur Beweisicherungskette
   - 2.3 Identifizierung
   - 2.4 Auswertung
   - 2.5 Präsentation

3. Arten von Computerkriminalität
   - 3.1 Kriminalität nach dem Gesetz
   - 3.2 Computerkriminalität
   - 3.3 Gerichtsbarkeit

4. Beweissammlung
   - 4.1 Software-Tools
   - 4.2 Hardware-Unterstützung
   - 4.3 Kryptographische Methoden zur Gewährleistung von Integrität und Beweissicherungskette
   - 4.4 Schritte für die Tatortsuche
   - 4.5 Überlegungen zum Cloud Computing
   - 4.6 SSD-spezifische Überlegungen
   - 4.7 Überlegungen zu mobilen Geräten
   - 4.8 E-Mail-Überlegungen
   - 4.9 Verschlüsselte Dateisysteme

5. System-Forensik
   - 5.1 Speicher-Analyse
   - 5.2 Prozessdumps und Analyse
   - 5.3 Windows-Forensik
   - 5.4 Linux-Forensik
   - 5.5 Mac OS-X-Forensik
   - 5.6 Apple iOS-Forensik
   - 5.7 Cloud-Forensik
   - 5.8 Website Forensik

6. Sandboxing-Malware
   - 6.1 Kommerzielle und Open-Source-Tools
   - 6.2 Beispiel: Cuckoo-Sandbox
   - 6.3 Überlegungen zum Gast-System
   - 6.4 „Spoonfeeding“ von unwilliger, langsamer oder verzögerter Malware
   - 6.5 Lesen von Sandbox-Berichten
   - 6.6 Sandbox als Teil der Operationen

7. Prinzipien des Reverse Engineering
   - 7.1 Reinraum-Umgebung
   - 7.2 Maschinencode
   - 7.3 Prinzipien der Demontage
   - 7.4 Dekompilierung
   - 7.5 Worauf Sie achten sollten
   - 7.6 Betriebssystem-Interaktionen
   - 7.7 Verwendung von IDA-Pro
   - 7.8 Verwendung von Ghidra

8. Auswertung
   - 8.1 Verbindungen herstellen
   - 8.2 Ursachensuche
   - 8.3 Mapping auf Mitre ATT&CK® Techniken, Taktiken und Verfahren
   - 8.4 Vermeidung vorschneller Urteile

9. Präsentation
   - 9.1 Bericht eschreiben
   - 9.2 Zusammenarbeit bei der Strafverfolgung
   - 9.3 Vorbereitung für die Präsentation vor Gericht
   - 9.4 Vorbereitung für die Präsentation beim Management

Literatur

Pflichtliteratur

Weiterführende Literatur

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing, Cham.
- Mitre ATT&CK®. https://attack.mitre.org/
- Newman, R. C. (2007): Computer Forensics: Evidence Collection and Management. Auerbach Publications, Boca Raton, FL.
- Reddy, N. (2019): Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations. Apress, New York City, NY.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: https://beginners.re/ (last accessed: 24 August 2020).

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBCSEHSF01_D

Artificial Intelligence

Modulcode: DLBDSEAIS1_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Artificial Intelligence)

Kurse im Modul

- Artificial Intelligence (DLBDSEAIS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Artificial Intelligence

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Artificial Intelligence

Kurscode: DLBDSEAIS01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Bestärkendes Lernen
   - 3.1 Was ist bestärkendes Lernen?
   - 3.2 Markov-Ketten und Wertfunktion
   - 3.3 Zeitdifferenz und Q-Lernen

4. Verarbeitung natürlicher Sprache (NLP)
   - 4.1 Einführung in NLP und Anwendungsbereiche
   - 4.2 Grundlegende NLP-Techniken
   - 4.3 Vektorisierung von Daten

5. Computer Vision
   - 5.1 Pixel und Filter
   - 5.2 Feature-Erkennung
   - 5.3 Verzerrungen und Kalibrierung
   - 5.4 Semantische Segmentierung

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Standards der Informationssicherheit

Modulcode: DLBCSEISS_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Standards der Informationssicherheit)

Kurse im Modul

- Standards der Informationssicherheit (DLBCSEISS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Schriftliche Ausarbeitung: Fallstudie	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Standards der Informationssicherheit

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Standards der Informationssicherheit

Kurscode: DLBCSEISS01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Einführung in die Informationssicherheit
   - 1.1 Grundlegende Definitionen, Sicherheitskonzepte und Ziele der Informationssicherheit
   - 1.2 Standards und regulatorische Rahmenbedingungen
   - 1.3 Sicherheitsstandards: ISO 27000-Familie und BSI-Standards
   - 1.4 Informationssicherheits-Managementsystem (ISMS)

2. Initiieren eines Informationssicherheits-Managementsystems
   - 2.1 Initiale Aufstellung für ein ISMS
   - 2.2 Analyse des Unternehmens
   - 2.3 Analyse des bestehenden ISMS und Bestimmung des Reifegrades
   - 2.4 Definition des ISMS-Anwendungsbereichs und der Sicherheitsrichtlinien

3. Implementierung des Informationssicherheits-Managementsystems
   - 3.1 Risikobewertung
   - 3.2 Statement of Applicability (SoA)
   - 3.3 Definition der Organisationsstruktur für die Informationssicherheit
   - 3.4 Dokumentenmanagement und Kommunikationsplan
   - 3.5 Definition von Maßnahmen und Prozeduren

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

5. Verbesserung des Informationssicherheits-Managementsystems
   - 5.1 Betrachung von Herausforderungen und Abweichungen
   - 5.2 Kontinuierliche Verbesserung
   - 5.3 Korrektive und präventive Aktionspläne

6. Maßnahmen des Informationssicherheits-Managementsystems
   - 6.1 Allgemeiner Aufbau der Maßnahmen
   - 6.2 Maßnahmen aus dem ISO 27001 - Annex A
   - 6.3 Verwaltung von Maßnahmen
   - 6.4 Bewertung der Effektivität von Maßnahmen

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Fallstudie

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

DLBCSEISS01_D

5. Semester

Seminar: Aktuelle Themen in Computer Science

Modulcode: DLBCSSCTCS_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Seminar: Aktuelle Themen in Computer Science (DLBCSSCTCS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Schriftliche Ausarbeitung: Seminararbeit	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Seminar: Aktuelle Themen in Computer Science

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Seminar: Aktuelle Themen in Computer Science

Kurscode: DLBCSSCTCS01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Seminar

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Seminararbeit

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLBCSSCTCS01_D

Advanced Data Analysis

Modulcode: DLBDSEDA1_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Advanced Data Analysis)

Kurse im Modul

- Advanced Data Analysis (DLBDSEDA01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Advanced Data Analysis

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Advanced Data Analysis

Kurscode: DLBDSEDA01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

4. Social Network Mining
   - 4.1 Einführung in die Analytik der sozialen Medien
   - 4.2 "Ausbeutung" von gängigen Plattformen für soziale Medien

5. Tests und Experimente
   - 5.1 Praktische A/B-Prüfung
   - 5.2 Multivariate Tests
   - 5.3 Tests mit mehrarmigen Banditen Algorithmen

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBDSEDA01_D

Projekt: Data Analysis

Modulcode: DLBDSEDA2_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Projekt: Data Analysis)

Kurse im Modul

- Projekt: Data Analysis (DLBDSEDA02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Portfolio	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Projekt: Data Analysis

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Projekt: Data Analysis

Kurscode: DLBDSEDA02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Portfolio

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

Lehrmethoden

- ☐ Learning Sprints®
- ☐ Skript
- ☐ Vodcast
- ☐ Shortcast
- ☐ Audio
- ☐ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☑ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

DLBDSEDA02_D

Cloud Computing

Modulcode: DLBDSCC_D

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Cloud Computing)

Kurse im Modul

- Cloud Computing (DLBDSCC01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

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

Qualifikationsziele des Moduls

Cloud Computing

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Cloud Computing

Kurscode: DLBDSCC01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Serverloses Rechnen
   - 3.1 Einführung in Serverless Computing
   - 3.2 Vorteile
   - 3.3 Einschränkungen

4. Etablierte Cloud-Plattformen
   - 4.1 Google-Cloudplattform
   - 4.2 Amazon-Webdienste
   - 4.3 Microsoft Azure

5. Datenwissenschaft in der Cloud
   - 5.1 Google-Dienste für Datenwissenschaft und maschinelles Lernen
   - 5.2 Amazon Web Services für Datenwissenschaft und maschinelles Lernen
   - 5.3 Microsoft Azure für Datenwissenschaft und maschinelles Lernen

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

DLBDSCC01_D

IT-Sicherheitsberatung

Modulcode: DLBCSEEISC_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ keine ▪ DLBCSEEISC01_D oder DLBCSEEISC01_E	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Technische und betriebliche IT-Sicherheitskonzeptionen (DLBCSEEISC01_D)
- Projekt: Einsatz und Konfiguration von SIEM-Systemen (DLBCSEEISC02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Technische und betriebliche IT-Sicherheitskonzeptionen • Studienformat "Fernstudium": Klausur, 90 Minuten Projekt: Einsatz und Konfiguration von SIEM-Systemen • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Technische und betriebliche IT-Sicherheitskonzeptionen

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

Projekt: Einsatz und Konfiguration von SIEM-Systemen

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

Qualifikationsziele des Moduls

Technische und betriebliche IT-Sicherheitskonzeptionen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Projekt: Einsatz und Konfiguration von SIEM-Systemen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Technische und betriebliche IT-Sicherheitskonzeptionen

Kurscode: DLBCSEEISC01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Schutz-Profile
   - 2.1 Referenzarchitektur, Technologie und Netzwerkbetrieb
   - 2.2 Risikobewertung, Restrisiko und Risikomanagement
   - 2.3 Sicherheitsanforderungen und Schutzmaßnahmen
   - 2.4 Sicherheitsbewertung von IT-Sicherheitsprodukten
   - 2.5 Akkreditierung von IT-Systemen und Netzwerken

3. Systeme der Intrusion Detection
   - 3.1 Erkennungsstrategie,
   - 3.2 Datenquellen, Sensoren
   - 3.3 Analytik
   - 3.4 Indikatoren für Kompromittierungen

4. Netzwerk-Überwachung
   - 4.1 Systeme zum Schutz vor Bedrohungen
   - 4.2 Technologie drahtloser Sensornetzwerke
   - 4.3 Austausch von Bedrohungsinformationen

5. Sicherheitsinformationen und Ereignismanagement (SIEM)
   - 5.1 Technische und betriebliche Daten-Quellen
   - 5.2 DATA-Fusion
   - 5.3 Normverhalten von Netzwerken
   - 5.4 Analyse großer Datenmengen - Übertragung technischer Daten in operative Informationen
   - 5.5 IT- Sicherheitslage und Lagebewusstsein
   - 5.6 Strategien zur Reaktion auf Vorfälle und automatisierte Gegenmaßnahmen

6. IT-Sicherheitsevaluierung und -bewertung
   - 6.1 IT-Sicherheits-Metriken
   - 6.2 Bewertung der IT-Sicherheit

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt: Einsatz und Konfiguration von SIEM-Systemen

Kurscode: DLBCSEEISC02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSEEISC01_D oder DLBCSEEISC01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Social Engineering

Modulcode: DLBCSEESE_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ DLBCSEESE01_D oder DLBCSEESE01_E ▪ keine	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Social Engineering und Insider Threats (DLBCSEESE01_D)
- Projekt: Social Engineering (DLBCSEESE02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Social Engineering und Insider Threats • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Fallstudie Projekt: Social Engineering • Studienformat "Fernstudium": Projektpräsentation

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Social Engineering und Insider Threats

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

Projekt: Social Engineering

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

Qualifikationsziele des Moduls

Social Engineering und Insider Threats

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Projekt: Social Engineering

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Social Engineering und Insider Threats

Kurscode: DLBCSEESE01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Methoden des Social Engineering
   - 1.1 Phishing, Speer-Phishing
   - 1.2 Quid pro quo, Köder, Medienabwurf
   - 1.3 Scareware, CEO-Betrug
   - 1.4 Vorwände, Heckenschützen

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

3. Erkennung von Insider-Bedrohungen
   - 3.1 DATA Mining zur Erkennung von Insider-Bedrohungen,
   - 3.2 Umfassender Rahmen für die Aufdeckung und Reaktion auf Insider-Bedrohungen
   - 3.3 Werkzeuge zur Selbsteinschätzung für die Evaluierung,
   - 3.4 Organisatorisches Lernen
   - 3.5 Innovative Prozesse
   - 3.6 Anwendung von Methoden des maschinellen Lernens

4. Sicherheitspolitik und -vorschriften
   - 4.1 Organisatorischer Rahmen, Compliance, Verhaltenskodex
   - 4.2 Ausbildung
   - 4.3 System zur Reaktion auf Zwischenfälle
   - 4.4 Schutz von klassifizierten / sensiblen Informationen
   - 4.5 Passwort-Richtlinie
   - 4.6 Datenspeicherung und Zugriffsprofile
   - 4.7 Schnittstellenüberwachung und -regulierung (USB-Politik, ...)

5. Nationale und internationale Zusammenarbeit und Informationsaustausch.
   - 5.1 Zusammenarbeit mit Internet Service Providern (ISP) und Interessenvertretern der IT-Sicherheit
   - 5.2 Austauschplattformen und Foren für taktische Techniken und Verfahren (TTP's) und bewährte Praktiken
   - 5.3 Zusammenarbeit mit nationalen Sicherheitsbehörden

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Fallstudie

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

Projekt: Social Engineering

Kurscode: DLBCSEESE02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSEESE01_D oder DLBCSEESE01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Projektpräsentation

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

Lehrmethoden

- ☐ Learning Sprints®
- ☐ Skript
- ☐ Vodcast
- ☐ Shortcast
- ☐ Audio
- ☐ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☑ Prüfungsleitfaden
- ☐ Live Tutorium/Course Feed

Host Forensics

Module Code: DLBCSEEHF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEHSF01_E or DLBCSEHSF01_D ▪ DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E	BA	10	300 h

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

Module Coordinator

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

Contributing Courses to Module

- Static and Dynamic Malware Analysis (DLBCSEEHF01_E)
- Seminar: Sandbox Interpretation (DLBCSEEHF02_E)

Module Exam Type

Module Exam	Split Exam
	Static and Dynamic Malware Analysis • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Sandbox Interpretation • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Static and Dynamic Malware Analysis

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

Seminar: Sandbox Interpretation

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

Learning Outcomes

Static and Dynamic Malware Analysis

On successful completion, students will be able to

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

Seminar: Sandbox Interpretation

On successful completion, students will be able to

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

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

Static and Dynamic Malware Analysis

Course Code: DLBCSEEHF01_E

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

Course Description

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

Course Outcomes

On successful completion, students will be able to

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

Contents

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

4. Malware Classification
   - 4.1 Antivirus
   - 4.2 Virustotal
   - 4.3 Yara
   - 4.4 Clustering with PEID, TELFHASH, TLSH, SSDEEP, etc

5. Sandboxes
   - 5.1 Levels of interaction
   - 5.2 Instrumentation
   - 5.3 Online sandboxing services, Virustotal
   - 5.4 Scripting for sandboxes
   - 5.5 Corporate sandbox considerations

6. Reversing
   - 6.1 Unpacking, decrypting and de-obfuscation
   - 6.2 Debugging techniques
   - 6.3 Control flow analysis
   - 6.4 Library and system calls

7. Digging deeper
   - 7.1 Domain and IP information
   - 7.2 Analysis of Javascript code
   - 7.3 Memory forensics
   - 7.4 Kernel debugging rootkits
   - 7.5 Theoretical underpinnings of program analysis

Literature

Compulsory Reading

Further Reading

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

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Sandbox Interpretation

Course Code: DLBCSEEHF02_E

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

Course Description

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

Course Outcomes

On successful completion, students will be able to

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

Contents

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

Literature

Compulsory Reading

Further Reading

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

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBCSEEHF02_E

DevSecOps

Modulcode: DLBCSEEDSO_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ IWNF01 oder IWNF01_E ▪ keine	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Techniken und Methoden der agilen Softwareentwicklung (IWNF01)
- Projekt: Agiles DevSecOps-Software-Engineering (DLBCSEEDSO01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Techniken und Methoden der agilen Softwareentwicklung • Studienformat "Fernstudium": Klausur, 90 Minuten Projekt: Agiles DevSecOps-Software-Engineering • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Techniken und Methoden der agilen Softwareentwicklung

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

Projekt: Agiles DevSecOps-Software-Engineering

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

Qualifikationsziele des Moduls

Techniken und Methoden der agilen Softwareentwicklung

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Projekt: Agiles DevSecOps-Software-Engineering

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Techniken und Methoden der agilen Softwareentwicklung

Kurscode: IWNF01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Agiles Portfolio- und Projektmanagement
   - 3.1 Planungsebenen im agilen Projektmanagement
   - 3.2 Agiles Portfoliomanagement
   - 3.3 Organisation mehrerer Teams in einem Projekt
   - 3.4 Produkt- und Release-Planung

4. Agiles Anforderungs- und IT-Architekturmanagement
   - 4.1 Requirements Engineering in agilen Projekten
   - 4.2 Architekturmanagement in agilen Projekten

5. Agiles Testen
   - 5.1 Grundlagen und Anforderungen an die QS-Organisation
   - 5.2 Teststufen und Agilität
   - 5.3 Testautomatisierung

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt: Agiles DevSecOps-Software-Engineering

Kurscode: DLBCSEEDSO01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IWNF01 oder IWNF01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLBCSEEDSO01_D

Sicherheit in komplexen Netzwerken

Modulcode: DLBCSEESCN_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	IAMG01 oder DLBCSEITPAM02	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Tobias Brückmann (IT-Architekturmanagement) / N.N. (Projekt: IT-Sicherheitsarchitekturen)

Kurse im Modul

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

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	IT-Architekturmanagement • Studienformat "Fernstudium": Klausur, 90 Minuten Projekt: IT-Sicherheitsarchitekturen • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

IT-Architekturmanagement

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

Projekt: IT-Sicherheitsarchitekturen

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

Qualifikationsziele des Moduls

IT-Architekturmanagement

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Projekt: IT-Sicherheitsarchitekturen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

IT-Architekturmanagement

Kurscode: IAMG01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Grundlagen und Begriffe zum Management von IT-Unternehmensarchitekturen
   - 1.1 IT-Unternehmensarchitektur
   - 1.2 Ziele von Enterprise Architecture Management
   - 1.3 Prozesse im Management von IT-Unternehmensarchitekturen

2. IT-Anwendungsportfoliomanagement
   - 2.1 Überblick über das IT-Anwendungsportfoliomanagement
   - 2.2 Anwendungshandbuch
   - 2.3 Portfolioanalyse
   - 2.4 Bebauungsplanung

3. Architektur-Governance
   - 3.1 Aufbauorganisation
   - 3.2 Entwicklung und Durchsetzung von Richtlinien
   - 3.3 Projektbegleitung

4. Modellierung von IT-Unternehmensarchitekturen
   - 4.1 Modelle im Kontext IT-Architekturmanagement
   - 4.2 Dokumentationsformen für Prozesse und Anwendungen
   - 4.3 Dokumentationsformen für Systeme und Technologien

5. Frameworks am Beispiel von TOGAF
   - 5.1 Grundlagen und Einsatz von IT-Architekturframeworks
   - 5.2 Überblick und Kategorien von EAM-Frameworks
   - 5.3 The Open Group Architecture Framework (TOGAF)

6. Referenzmodelle und Musterkataloge
   - 6.1 Referenzmodelle für Architekturen
   - 6.2 Musterkatalog für Gestaltung von EAM

Literatur

Pflichtliteratur

Weiterführende Literatur

- Hanschke, I. (2011): Enterprise Architecture Management. Einfach und effektiv. Hanser, München.
- Keller, W. (2012): IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung. 2. Auflage, dpunkt.verlag, Heidelberg.
- Keuntje. J. H./Barkow, R. (Hrsg.) (2010): Enterprise Architecture. Management in der Praxis. Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen.
- Ross, J. W./ Weill, P./Robertson, D. C. (2006): Enterprise Architecture as Strategy. Creating a Foundation for Business Execution. Harvard Business Review Press, Boston.
- Schwarzer, B. (2009): Einführung in das Enterprise Architecture Management. Verstehen – Planen – Umsetzen. Books on Demand, Norderstedt.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt: IT-Sicherheitsarchitekturen

Kurscode: DLBCSEESCN01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IAMG01 oder DLBCSEITPAM02

Beschreibung des Kurses

Unter Verwendung von Methoden und Techniken aus dem Bereich IT-Architekturmanagement bearbeiten die Studierenden in diesem Kurs selbständig eine praktische Fragestellung im Bereich der IT-Sicherheitsarchitektur. Am Ende des Kurses sind die Studierenden in der Lage, auf der Basis einer bestehenden IT-System- / Netzwerkarchitektur eine IT-Sicherheitsarchitektur selbstständig zu entwickeln.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

- Umsetzung und Dokumentation praktischer Fragen zur IT-Sicherheit im Rahmen des IT-Architekturmanagements. Typische Szenarien sind z.B. "Implementierung von IT-Sicherheitsgeräten in komplexen Netzwerken", "Gestaltung von Prozessen für Sicherheitsupdates und Patch-Management" und "Einsatz von Inhouse-Ressourcen oder Outsourcing von IT-Sicherheitsaufgaben".

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Bartsch, M. / Frey, S. (2014): Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Fachmedien, Wiesbaden. ▪ Müller, K.-R. (2014): IT-Sicherheit mit System. 5. Auflage, Springer Fachmedien, Wiesbaden. ▪ Pfister, M. (2019): Info Guard Swiss Cyber Security - In 3 einfachen (aber wichtigen) Schritten zur Enterprise IT-Sicherheitsarchitektur. (URL: www.infoguard.ch [zuletzt besucht am 22.08.2020]).

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Network Forensics

Module Code: DLBCSEENF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E ▪ DLBCSEINF01_E or DLBCSEINF01_D	BA	10	300 h

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

Module Coordinator

N.N. (Protocols, Log- and Dataflow-Analysis in Depth) / N.N. (Seminar: Threat Hunting, Analysis and Incident Response)

Contributing Courses to Module

- Protocols, Log- and Dataflow-Analysis in Depth (DLBCSEENF01_E)
- Seminar: Threat Hunting, Analysis and Incident Response (DLBCSEENF02_E)

Module Exam Type

Module Exam	Split Exam
	Protocols, Log- and Dataflow-Analysis in Depth • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Threat Hunting, Analysis and Incident Response • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Protocols, Log- and Dataflow-Analysis in Depth

- Introduction
- Basic protocol layering
- Operating system logs
- HTTP server
- IP Firewall
- Web application filter
- Authentication servers
- Databases
- Intrusion Detection and Protection System (IDPS)
- Email systems
- Content filters
- SSH
- Less common systems
- Context
- Log management Infrastructure
- Security Information and Event Management (SIEM)
- Visualization
- Security Operations Centers (SOC)
- Logging in the cloud
- Dataflow monitoring
- Attacks against logging
- Analysis techniques
- Reporting

Seminar: Threat Hunting, Analysis and Incident Response

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

Learning Outcomes

Protocols, Log- and Dataflow-Analysis in Depth

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Seminar: Threat Hunting, Analysis and Incident Response

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

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

Protocols, Log- and Dataflow-Analysis in Depth

Course Code: DLBCSEENF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D

Course Description

Logging is done for a variety of diagnosis reasons, but these logs can be very useful in finding security incidents. In this course, we look at a variety of sources of log files. These range from operating system logs, to application logs and network traffic logs. Context and additional information also need to be collected. All this data is then consolidated in a Security Information and Event Management system where it can be analyzed and triaged for action. Finally, major incidents need to be documented and communicated to the relevant parties.

Course Outcomes

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Contents

1. Introduction
   - 1.1 Network protocols
   - 1.2 Applications of log files
   - 1.3 Operating system log files
   - 1.4 Application log files
   - 1.5 Network log files
   - 1.6 Dataflow logs
   - 1.7 Security log files

2. Basic protocol layering
   - 2.1 Internet protocol hierarchy
   - 2.2 TCP connection
   - 2.3 Frame layer
   - 2.4 Ethernet layer
   - 2.5 Internet Protocol layer
   - 2.6 Transport Control Protocol
   - 2.7 UDP packets
   - 2.8 TCP/IP in relation to the OSI layer model
   - 2.9 Reading RFCs and related documentation

3. Operating system logs
   - 3.1 Syslog
   - 3.2 System events
   - 3.3 Audit events

4. HTTP server
   - 4.1 Common server vendors
   - 4.2 Apache log format
   - 4.3 Web edge logging
   - 4.4 Logs from Content delivery networks

5. IP Firewall

6. Web application filter

7. Authentication servers

8. Databases

9. Intrusion Detection and Protection System (IDPS)

10. Email systems
    - 10.1 SMTP
    - 10.2 POP
    - 10.3 Exchange

11. Content filters
    - 11.1 Spam and Phish filters
    - 11.2 Malware filters
    - 11.3 Data leak prevention
12. SSH
13. Less common systems
    - 13.1 MQTT
    - 13.2 CoAP
    - 13.3 XMPP
    - 13.4 BGP
    - 13.5 RIP
    - 13.6 DNS
14. Context
    - 14.1 Asset management
    - 14.2 Known vulnerable systems
    - 14.3 Network topology
15. Log management Infrastructure
    - 15.1 Log generation
    - 15.2 Storage
    - 15.3 Analysis
    - 15.4 Monitoring
    - 15.5 Security and privacy of logs
    - 15.6 Roles and responsibility
    - 15.7 Policies
    - 15.8 Long term log storage
16. Security Information and Event Management (SIEM)
17. Visualization
18. Security Operations Centers (SOC)
19. Logging in the cloud
20. Dataflow monitoring

21. Attacks against logging

22. Analysis techniques
    - 22.1 Entry Normalization
    - 22.2 Semantics of log events
    - 22.3 Prioritizing entries
    - 22.4 Aggregation
    - 22.5 Rule based systems
    - 22.6 Anomaly detection
    - 22.7 Machine learning
    - 22.8 Triaging incidents
    - 22.9 Working with filters

23. Reporting
    - 23.1 Indicators of compromise
    - 23.2 Mapping to the Mitre ATT&CK framework
    - 23.3 STIX, TAXII
    - 23.4 Written reports and presentations

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- NIST Special Publicaton 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Threat Hunting, Analysis and Incident Response

Course Code: DLBCSEENF02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E

Course Description

Much of a security officer's work is with data where incidents need to be analyzed and countermeasures implemented. This course uses the Mitre ATT&CK® framework to reference TTPs (Techniques, Tactics and Procedures) that map to security events. Not all TTPs can be found in labeled security events, so Threat Hunting aims to go beyond ordinary incident response and find indicators of these TTPs also using other methods.

Course Outcomes

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Contents

- In this seminar, we cover the subjects of incident response and threat hunting using the Mitre ATT&CK® framework and publicly available reports.

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

6. Semester

Business Intelligence

Modulcode: IWBI

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Dr. Peter Poensgen (Business Intelligence) / Dr. Peter Poensgen (Projekt Business Intelligence)

Kurse im Modul

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

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Business Intelligence • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "Kombistudium": Klausur, 90 Minuten Projekt Business Intelligence • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Business Intelligence

- Motivation und Begriffsbildung
- Datenbereitstellung
- Data Warehouse
- Modellierung multidimensionaler Datenräume
- Analysesysteme
- Distribution und Zugriff

Projekt Business Intelligence

Mögliche Themengebiete für das BI-Projekt sind u.a. „Management von BI-Projekten, „Konzeption von multidimensionalen Datenmodellen“ sowie „Prototypische Umsetzung von kleinen BI-Anwendungen“.

Qualifikationsziele des Moduls

Business Intelligence

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivation, Anwendungsfälle und Grundlagen für Business Intelligence zu erklären.
- Techniken und Methoden zur Bereitstellung und Modellierung von Daten sowie für BI relevante Arten von Daten zu benennen und zu erläutern sowie voneinander abzugrenzen.
- Techniken und Methoden zur Informationsgenerierung und -speicherung zu erläutern und auf Basis konkreter Anforderungen selbstständig geeignete Methoden auszuwählen.

Projekt Business Intelligence

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine Lösung zu einer praktischen Fragestellung im Thema Business Intelligence zu konzipieren, prototypisch umzusetzen und die dabei erzielten Ergebnisse zu dokumentieren.
- typische Probleme und Herausforderungen in der Konzeption und praktischen Umsetzung kleiner BI-Lösungen zu benennen und zu erläutern.

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

Business Intelligence

Kurscode: IWBI01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Business Intelligence (BI) dient der Gewinnung von Informationen aus Unternehmensdaten, die sowohl für eine gezielte Unternehmenssteuerung als auch für die Optimierung von Geschäftsaktivitäten relevant sind. Im Rahmen dieses Kurses werden Techniken, Vorgehensweisen und Modelle zur Datenbereitstellung, Informationsgenerierung und -analyse sowie der Verteilung der gewonnenen Informationen vorgestellt und diskutiert. Sie werden danach in der Lage sein, die verschiedenen Themengebiete des Data Warehousing zu erläutern und Methoden bzw. Techniken für konkrete Anforderungen selbstständig auszuwählen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivation, Anwendungsfälle und Grundlagen für Business Intelligence zu erklären.
- Techniken und Methoden zur Bereitstellung und Modellierung von Daten sowie für BI relevante Arten von Daten zu benennen und zu erläutern sowie voneinander abzugrenzen.
- Techniken und Methoden zur Informationsgenerierung und -speicherung zu erläutern und auf Basis konkreter Anforderungen selbstständig geeignete Methoden auszuwählen.

Kursinhalt

1. Motivation und Begriffsbildung
   - 1.1 Motivation und historische Entwicklung
   - 1.2 BI als Rahmenwerk
2. Datenbereitstellung
   - 2.1 Operative und dispositive Systeme
   - 2.2 Das Data-Warehouse-Konzept
   - 2.3 Architekturvarianten
3. Data Warehouse
   - 3.1 ETL-Prozess
   - 3.2 DWH und Data Mart
   - 3.3 ODS und Metadaten

4. Modellierung multidimensionaler Datenräume
   - 4.1 Datenmodellierung
   - 4.2 OLAP-Würfel
   - 4.3 Physische Speicherung
   - 4.4 Star- und Snowflake-Schema
   - 4.5 Historisierung

5. Analysesysteme
   - 5.1 Freie Datenrecherche und OLAP
   - 5.2 Berichtssysteme
   - 5.3 Modellgestützte Analysesysteme
   - 5.4 Konzeptorientierte Systeme

6. Distribution und Zugriff
   - 6.1 Informationsdistribution
   - 6.2 Informationszugriff

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bachmann, R./Kemper, G. (2011): Raus aus der BI-Falle. Wie Business Intelligence zum Erfolg wird. 2. Auflage, mitp, Heidelberg.
- Bauer, A./Günzel, H. (2008): Data Warehouse Systeme. Architektur, Entwicklung, Anwendung. 3. Auflage, dpunkt.verlag, Heidelberg.
- Betz, R. (2015): Werde Jäger des verlorenen Schatzes. In: Immobilienwirtschaft, Heft 5, S. 1614–1164. (URL https://www.haufe.de/download/immobilienwirtschaft-ausgabe-052015-immobilienwirtschaft-fachmagazin-fuer-management-recht-praxis-303530.pdf [letzter Zugriff: 27.02.2017]).
- Bodendorf, F. (2006): Daten- und Wissensmanagement. 2. Auflage, Springer, Berlin.
- Chamoni, P./Gluchowski, P. (Hrsg.) (2006): Analytische Informationssysteme Business Intelligence-Technologien und -Anwendungen. Springer, Berlin.
- Engels, C. (2008): Basiswissen Business Intelligence. W3L, Herdecke/Witten.
- Gansor, T./Totok, A./Stock, S. (2010): Von der Strategie zum Business Intelligence Competency Center (BICC). Konzeption – Betrieb – Praxis. Hanser, München.
- Gluchowski, P./Gabriel, R./Dittmar, C. (2008): Management Support Systeme und Business Intelligence. Computergestützte Informationssysteme für Fach- und Führungskräfte. 2. Auflage, Springer, Berlin/Heidelberg.
- Grothe, M. (2000): Business Intelligence. Aus Informationen Wettbewerbsvorteile gewinnen. Addison-Wesley, München.
- Gutenberg, E. (1983): Grundlagen der Betriebswirtschaft, Band 1. Die Produktion. 18. Auflage, Springer, Berlin/Heidelberg/New York.
- Hannig, U. (Hrsg.) (2002): Knowledge Management und Business Intelligence. Springer, Berlin.
- Hansen, H.-R./Neumann, G. (2001): Wirtschaftsinformatik I. Grundlagen betrieblicher Informationsverarbeitung. 8. Auflage, Lucius & Lucius UTB, Stuttgart.
- Humm, B./Wietek, F. (2005): Architektur von Data Warehouses und Business Intelligence Systemen. In: Informatik Spektrum, S. 3–14. (URL: https://www.fbi.h-da.de/fileadmin/personal/b.humm/Publikationen/Humm__Wietek_-_Architektur_DW__Informatik-Spektrum_2005-01_.pdf [letzter Zugriff: 27.02.2017]).
- Kemper, H.-G./Baars, H./Mehanna, W. (2010): Business Intelligence – Grundlagen und praktische Anwendungen. Eine Einführung in die IT-basierte Managementunterstützung. 3. Auflage, Vieweg+Teubner, Stuttgart.
- Turban, E. et al. (2010): Business Intelligence. A Managerial Approach. 2. Auflage, Prentice Hall, Upper Saddle River (NJ).

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☐ Live Tutorium/Course Feed

Projekt Business Intelligence

Kurscode: IWBI02

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Unter Anwendung bekannter Methoden und Techniken aus dem Themengebiet Business Intelligence bearbeiten die Studierenden in diesem Kurs selbstständig eine praktische Fragestellung.Zum Abschluss des Kurses können Sie selbstständig auf der Grundlage konkreter Anforderungen Business Intelligence-Anwendungen konzipieren und prototypisch umsetzen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine Lösung zu einer praktischen Fragestellung im Thema Business Intelligence zu konzipieren, prototypisch umzusetzen und die dabei erzielten Ergebnisse zu dokumentieren.
- typische Probleme und Herausforderungen in der Konzeption und praktischen Umsetzung kleiner BI-Lösungen zu benennen und zu erläutern.

Kursinhalt

- Umsetzung und Dokumentation von praktischen Fragestellungen zum Einsatz von Business Intelligence-Anwendungen. Typische Szenarien sind beispielsweise „Management von BI-Projekten“, „Konzeption von multidimensionalen Datenmodellen“ und „Prototypische Umsetzung von kleinen BI-Anwendungen“.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Brenner, W./Uebernickel, F. (2015): Design Thinking. Das Handbuch. Frankfurter Allgemeine Buch, Frankfurt a. M.
- Brown, T. (2008): Design Thinking. In: Harvard Business Review, Heft Juni, S. 84–95.
- Meinel, C./Weinberg, U./Krohn, T. (Hrsg.) (2015): Design Thinking Live. Wie man Ideen entwickelt und Probleme löst. Murmann, Hamburg.
- Uebernickel, F./Brenner, W. (2016): Design Thinking. In: Hoffmann, C. P. et al. (Hrsg.): Business Innovation: Das St. Galler Modell. Springer, Wiesbaden, S. 243–265.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Future Threats

Modulcode: DLBCSEEFT_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ IREN01 oder DLBCSRE01; DLBCSEEFT01_D oder DLBCSEEFT01_E ▪ IREN01 oder DLBCSRE01	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Threat Modeling) / N.N. (Projekt: Threat Modeling)

Kurse im Modul

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

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Threat Modeling

- C.I.A. Denken und mehr
- Messung der Cyber-Bedrohung
- Modellierung von Bedrohungen
- Bibliotheken angreifen
- Regeln, Vorschriften und Strafverfolgung
- Risiko-Management
- Threat Mitigation

Projekt: Threat Modeling

Dieser Kurs behandelt die Theorie und Praxis des Auffindens und der Modellierung von Bedrohungen in einem bestimmten System, einer bestimmten Architektur oder einem bestimmten Szenario. Er behandelt Methoden und Quellen für übliche Bedrohungsmuster. In einem Projekt wird die Theorie in die Praxis umgesetzt, indem eine gegebene Situation auf Bedrohungen analysiert wird.

Qualifikationsziele des Moduls

Threat Modeling

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- souverän mögliche Bedrohungsarten zu durchdenken.
- diese Bedrohungen mit Hilfe einer gebräuchlichen Modellierungsmethode zu modellieren.
- relevante Techniken, Taktiken und Verfahren in Bezug auf ein bestimmtes Szenario zu finden.
- das aus dem Bedrohungsmodell hervorgehende Risiko zu ermitteln.
- das Risiko durch die Implementierung von Änderungen des Designs zu mindern.

Projekt: Threat Modeling

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihr Wissen über die Modellierung von Bedrohungen auf Fälle und Szenarien anzuwenden.
- ihr daraus resultierendes Modell auf der Grundlage einer soliden Argumentation und in Bezug auf bekannte Techniken, Taktiken und Verfahren der Angreifer zu rechtfertigen.
- einen Bericht zu verfassen, der ihre Argumentation in systematischer und verständlicher Weise darlegt.

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

Threat Modeling

Kurscode: DLBCSEEFT01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01

Beschreibung des Kurses

Wenn ein System oder eine Architektur geschaffen wird, ist es wichtig, dass mögliche Bedrohungen gleichzeitig bewertet werden. Durch die Verwendung sowohl von Modellierungsmethoden als auch von in der Vergangenheit beobachteten Angriffsmustern ist es möglich, ein neues oder bestehendes System auf Bedrohungen hin zu untersuchen. Aus dieser Analyse lassen sich Risiken und Maßnahmen zu deren Verminderung ableiten. Während die gebräuchlichsten Methoden auf den Angriffsbäumen und dem STRIDE-Modell basieren, werden bei der Angriffsmodellierung in letzter Zeit auch Repositorien von Angreifer-Techniken, -Taktiken und -Verfahren (TTP´s) zur Inspiration herangezogen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- souverän mögliche Bedrohungsarten zu durchdenken.
- diese Bedrohungen mit Hilfe einer gebräuchlichen Modellierungsmethode zu modellieren.
- relevante Techniken, Taktiken und Verfahren in Bezug auf ein bestimmtes Szenario zu finden.
- das aus dem Bedrohungsmodell hervorgehende Risiko zu ermitteln.
- das Risiko durch die Implementierung von Änderungen des Designs zu mindern.

Kursinhalt

1. C.I.A. Denken und mehr
   - 1.1 Vertraulichkeit (Confidentiality)
   - 1.2 Integrität (Integrity)
   - 1.3 Verfügbarkeit (Availability)
   - 1.4 Sicherheit und andere Belange
2. Messung der Cyber-Bedrohung
   - 2.1 Messung und Verwaltung
   - 2.2 Metriken zur Cyber-Bedrohung
   - 2.3 Messung der Bedrohung für eine Organisation
   - 2.4 Die Wahrscheinlichkeit größerer Cyber-Angriffe
   - 2.5 Black Swan events

3. Modellierung von Bedrohungen
   - 3.1 Methodik des Angrifssbaumes
   - 3.2 STRIDE
   - 3.3 DREAD
   - 3.4 Schmerzpyramide – “Pyramid of Pain”

4. Bibliotheken angreifen
   - 4.1 CAPEC
   - 4.2 Soloves Taxonomie der Privatsphäre
   - 4.3 Modellierung mit Mitre ATT&CK®
   - 4.4 Identifizierung neuer Arten von Angriffen

5. Regeln, Vorschriften und Strafverfolgung
   - 5.1 Cyber-Gesetze
   - 5.2 Compliance und Strafverfolgung

6. Risiko-Management
   - 6.1 Veränderte Herangehensweisen an das Risikomanagement
   - 6.2 Reaktion auf Zwischenfälle und Krisenmanagement
   - 6.3 Berücksichtigung der Black Swan Events
   - 6.4 Kontinuierliche Neubewertung

7. Threat Mitigation
   - 7.1 Defensive Taktiken und Technologien
   - 7.2 Strategien zur Risikominderung
   - 7.3 Validierung des Abwehrschutzes
   - 7.4 Sicherheit und Privacy by Design
   - 7.5 Implementierung von Mechanismen zur Verminderung der Bedrohungen in einer Organisation

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ CAPEC: Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/ ▪ Kim, P. (2014): The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2015): The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2018): The Hacker Playbook 3: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Mitre ATT&CK®. https://attack.mitre.org/ ▪ Pfleeger, C. P. / Pfleeger, S. L. / Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London. ▪ Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☑ Vodcast	☐ Prüfungsleitfaden
☐ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt: Threat Modeling

Kurscode: DLBCSEEFT02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01; DLBCSEEFT01_D oder DLBCSEEFT01_E

Beschreibung des Kurses

Die Bedrohungen für moderne Computersysteme sind vielfältig und entwickeln sich ständig weiter. In diesem Projekt hat der Studierende die Gelegenheit, die Kunst und Wissenschaft der Bedrohungsmodellierung auf ein Szenario anzuwenden, das vom Dozenten zusammen mit dem Studierenden definiert wird. Die Grundlage bilden reale oder fiktive Fallstudien, zu denen der Studierende unter Verwendung einer geeigneten Methodik die Bedrohungen identifizieren und darüber berichten soll. Diese kann aus Methoden wie Attack Trees, STRIDE, DREAD oder einer gerechtfertigten Aufzählung von CAPEC oder Mitre ATT&CK® TTPs ausgewählt werden, je nachdem, was der Kursteilnehmer für am geeignetsten hält. Die Ergebnisse werden in Form eines Berichts präsentiert.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihr Wissen über die Modellierung von Bedrohungen auf Fälle und Szenarien anzuwenden.
- ihr daraus resultierendes Modell auf der Grundlage einer soliden Argumentation und in Bezug auf bekannte Techniken, Taktiken und Verfahren der Angreifer zu rechtfertigen.
- einen Bericht zu verfassen, der ihre Argumentation in systematischer und verständlicher Weise darlegt.

Kursinhalt

- Für einen bestimmten Fall oder ein bestimmtes Szenario modellieren Studierende die Bedrohungen unter Verwendung einer etablierten Methodik und reicht dann den Bericht und, falls zutreffend, alle Codes und Daten ein. Spezifische Probleme und Kontexte werden vom Tutor vorgegeben, Vorschläge der Studierenden können jedoch berücksichtigt werden.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Case Studies (Cyber): https://www.securitymagazine.com/topics/2664-case-studies-cyber ▪ Karger, P. A. / Scherr, R. R. (1974): MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS. ▪ Palmer, C. C. (2001): Ethical Hacking.IBM Systems Journal. 40 (3):769. ▪ Shostack, A. 2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ. ▪ Van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLBCSEEFT02_D

Cloud Security

Module Code: DLBCSEECS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBDSCC01 or DLBDSCC01_D ▪ DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E	BA	10	300 h

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

Module Coordinator

N.N. (Security Controls in the Cloud) / N.N. (Project: Security by Design in the Cloud)

Contributing Courses to Module

- Security Controls in the Cloud (DLBCSEECS01_E)
- Project: Security by Design in the Cloud (DLBCSEECS02_E)

Module Exam Type

Module Exam	Split Exam
	Security Controls in the Cloud • Study Format "Distance Learning": Exam, 90 Minutes Project: Security by Design in the Cloud • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Security Controls in the Cloud

- Cloud security
- Losing the intranet
- Security by design
- Secure cloud coding
- Confidentiality aspects
- Monitoring and Audit

Project: Security by Design in the Cloud

This module is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Learning Outcomes

Security Controls in the Cloud

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Project: Security by Design in the Cloud

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

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

Security Controls in the Cloud

Course Code: DLBCSEECS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D

Course Description

Maintaining a datacenter is expensive and inflexible, so it is expected that most corporations will be moving their server-based processes to a private, public or hybrid cloud in the next few years. Doing so will make operations more flexible and elastic but poses challenges to security architectures and operations. The paradigm of Infrastructure as Code (IaC) has been embraced by cloud providers and is a great opportunity to architect security into the design of a system (security by design) utilizing security best practices. However, too often, we see the on-premises mentality being applied to cloud deployments resulting in less secure systems instead of utilizing the security advantages a cloud provides. This course teaches the principles of Cloud Native security and how to avoid common pitfalls.

Course Outcomes

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Contents

1. Cloud security is different
   - 1.1 Shared responsibility model
   - 1.2 Infrastructure as code
   - 1.3 The Private, Public and Hybrid Cloud
   - 1.4 Types of virtualization
   - 1.5 Cloud threat models: Mitre Cloud ATT&CK

2. Losing the intranet
   - 2.1 Identify and Access Management
   - 2.2 Principle of least privilege and fine-grained cloud access control
   - 2.3 Using Software Defined Networks, virtual private clouds and subnets
   - 2.4 Moving to a serverless architecture
   - 2.5 Defense in depth

3. Security by design
   - 3.1 Orchestration: Infrastructure as Code
   - 3.2 The Automate-Everything principle, Updating and Repeatability
   - 3.3 Reuse of good design patterns
   - 3.4 Container security
   - 3.5 Identification and Authentication

4. Secure cloud coding
   - 4.1 Software supply chain security
   - 4.2 Continuous Integration and Deployment
   - 4.3 Testing in code integration for security
   - 4.4 Canaries in code deployment
   - 4.5 Policy engines

5. Confidentiality aspects
   - 5.1 Secrets management
   - 5.2 Encryption of data at rest
   - 5.3 Encryption of data in transit
   - 5.4 Data leakage and exfiltration

6. Availability
   - 6.1 Storage tiers and locality
   - 6.2 Backup strategies
   - 6.3 Data and process redundancy
   - 6.4 Data lifecycle configuration
   - 6.5 DDoS mitigation

7. Locality
   - 7.1 Compliance requirements
   - 7.2 Geography of data/processes
   - 7.3 Redundancy of data centers
   - 7.4 Colocation for performance reasons

8. Monitoring and Audit
   - 8.1 Centralized logging
   - 8.2 Auditing orchestration scripts
   - 8.3 Detecting misconfigurations
   - 8.4 Cloud Forensics

9. Summary and Research topics
   - 9.1 Homomorphic encryption
   - 9.2 Attestation
   - 9.3 Proof-carrying data
   - 9.4 Side-channel attacks
   - 9.5 Conclusions

Literature

Compulsory Reading

Further Reading

- Mitre Cloud ATT&CK. https://attack.mitre.org/matrices/enterprise/cloud/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Security by Design in the Cloud

Course Code: DLBCSEECS02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E

Course Description

This course provides the opportunity to implement a cloud software system using best cloud security practices. A list of ideas is provided on the online learning platform. In addition, the students can contribute use case ideas of their own after consulting with the tutor. The core aim is to apply the theoretical knowledge of cloud security methods and best practices to implement an application that is deployed as an Infrastructure-as-code project, can be monitored and audited, as well as easily and preferably automatically updated without danger. This entails reasoning about possible design and architectural choices in a rational way, as well as implementing them on a cloud platform, such as CNCF, Amazon AWS, Microsoft Azure or Google GCP.

Course Outcomes

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Contents

- This course is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Literature

Compulsory Reading

Further Reading

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Pentesting

Module Code: DLBCSEEPT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D ▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E	BA	10	300 h

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

Module Coordinator

N.N. (Principles of Ethical Hacking) / N.N. (Project: Pentesting)

Contributing Courses to Module

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

Module Exam Type

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

Weight of Module
see curriculum

Module Contents

Principles of Ethical Hacking

- History of ethical hacking
- Ethical and legal frameworks
- Planning phase
- Social Engineering & OSINT
- Tools
- RATs, Rootkits and Command & Control
- Data exfiltration
- Red/Blue Teams
- Bug Bounty programs
- Report writing

Project: Pentesting

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system.

Learning Outcomes

Principles of Ethical Hacking

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Project: Pentesting

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

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

Principles of Ethical Hacking

Course Code: DLBCSEEPT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Ethical hacking is an essential part in testing security implementations as well as discovering overlooked security issues. In this course, we will look at the principles and tools that hackers use and how ethical hacking is effectively utilized.

Course Outcomes

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Contents

1. History of ethical hacking

2. Ethical and legal frameworks
   - 2.1 Certifications
   - 2.2 Defining parameters of engagement
   - 2.3 Contracts

3. Planning phase
   - 3.1 Using Mitre PreATT&CK® for reconnaissance
   - 3.2 User Mitre Enterprise ATT&CK® for tool selection
   - 3.3 Documentation

4. Social Engineering & OSINT

5. Tools
   - 5.1 Web application pentesting tools
   - 5.2 Remote execution testing tools
   - 5.3 Password cracking
   - 5.4 OSINT tools
   - 5.5 Fuzzing tools
6. RATs, Rootkits and Command & Control
7. Data exfiltration
8. Red/Blue Teams
9. Bug Bounty programs
10. Report writing

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Pentesting

Course Code: DLBCSEEPT02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E

Course Description

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system. Students write a report outlining the vulnerabilities found, the methods used and proposals for fixing that class of vulnerability.

Course Outcomes

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Contents

- The student will be provided with virtual environments emulating corporate systems and an attacker machine with the necessary tools.

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBCSEEPT02_E

Industrielle Systemsicherheit

Modulcode: DLBCSEEIST_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	DLBINGEIT01 oder DLBINGEIT01_E	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

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

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Grundlagen der industriellen Softwaretechnik

- Aufbau und Organisation von Informationssystemen
- Risiken und Herausforderungen der industriellen Softwaretechnik
- Softwarelebenszyklus: Von Planung bis Ablösung
- Requirements Engineering und Spezifikation
- Architektur und Implementierung
- Qualitätssicherung, Betrieb und Weiterentwicklung
- Rollen im Software Engineering
- Organisation von Softwareprojekten
- Softwareprozessmodell-Rahmenwerke

Sicherheit im Internet of Things

- Grundlagen des Internet der Dinge (IoT)
- Angriffe auf das Internet der Dinge
- Sicherheit durch Design
- Sichern von Geräten für das Internet der Dinge
- Operative Sicherheit
- Cloud-Sicherheit
- Große Daten / Künstliche Intelligenz

Qualifikationsziele des Moduls

Grundlagen der industriellen Softwaretechnik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einfache Berechnungen im Binärsystem (Boolsche Algebra) durchzuführen.
- den Aufbau von Rechnersystemen und Kommunikationsnetzen zu beschreiben.
- die Phasen eines SW-Lebenszyklus voneinander abzugrenzen.
- Rollen und Phasen im Software-Prozess voneinander abzugrenzen.
- verschiedene Vorgehensmodelle der SW-Entwicklung zu kennen.
- typische Herausforderungen und Risiken der industriellen SW-Entwicklung zu kennen.
- verschiedene Programmierparadigmen und deren Einsatz zu kennen.

Sicherheit im Internet of Things

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte von IoT-Architekturen zu kennen und zu verstehen.
- die gängigsten Schwachstellen, Bedrohungen und Risiken für das Internet der Dinge zu kennen und zu verstehen.
- Gegenmaßnahmen für IoT-Schwachstellen zu verstehen und anzuwenden.
- ein IoT-Architekturmodell/eine IoT-Lösung zu analysieren.

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

Grundlagen der industriellen Softwaretechnik

Kurscode: IGIS01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen Einblick in die technischen und theoretischen Grundlagen des Software Engineering zu vermitteln. Neben dem generellen Aufbau von Rechnersystemen werden den Studierenden typische Herausforderungen bei der Entwicklung industrieller Informationssysteme vermittelt. Darüber hinaus wird dargestellt, mit welchen typischen Phasen und Aktivitäten im Software Engineering diese Risiken gezielt adressiert werden.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einfache Berechnungen im Binärsystem (Boolsche Algebra) durchzuführen.
- den Aufbau von Rechnersystemen und Kommunikationsnetzen zu beschreiben.
- die Phasen eines SW-Lebenszyklus voneinander abzugrenzen.
- Rollen und Phasen im Software-Prozess voneinander abzugrenzen.
- verschiedene Vorgehensmodelle der SW-Entwicklung zu kennen.
- typische Herausforderungen und Risiken der industriellen SW-Entwicklung zu kennen.
- verschiedene Programmierparadigmen und deren Einsatz zu kennen.

Kursinhalt

1. Aufbau und Organisation von Informationssystemen
   - 1.1 0 und 1 als Grundlage aller IT-Systeme
   - 1.2 Von-Neumann-Architektur
   - 1.3 Verteilte Systeme und Kommunikationsnetze
   - 1.4 Betriebliche Informationssysteme
2. Risiken und Herausforderungen der industriellen Softwaretechnik
   - 2.1 Eigenschaften von industriellen Softwaresystemen
   - 2.2 Softwaretechnik
   - 2.3 Risiken und typische Probleme
   - 2.4 Ursachenforschung
   - 2.5 Herausforderungen im Software Engineering

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Gumm, H. P./Sommer, M. (2011): Einführung in die Informatik. 9. Auflage, Oldenbourg, München. ▪ Hansen, H. R./Neumann, G. (2009): Wirtschaftsinformatik 1. Grundlagen und Anwendungen. 10. Auflage, UTB, Stuttgart. ▪ Ludewig, J./Lichter, H. (2010): Software Engineering. Grundlagen, Menschen, Prozesse, Techniken. 2. Auflage, dpunkt.verlag, Heidelberg. ▪ Sommerville, I. (2007): Software Engineering. 8. Auflage, Addison-Wesley, Boston.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Sicherheit im Internet of Things

Kurscode: DLBCSEEIST01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBINGEIT01 oder DLBINGEIT01_E

Beschreibung des Kurses

Das Internet der Dinge (IoT) ist ein Megatrend. Er umfasst sowohl Endverbrauchersysteme als auch industrielle Systeme und Technologien (Industrial IoT, oder IIoT). Es gibt eine zunehmende Anzahl miteinander verbundener Geräte, aus denen sich das Internet der Dinge zusammensetzt. Im Allgemeinen besteht die Architektur des Internet der Dinge aus Endgeräten, Cloud-Lösungen und Akteuren/Sensoren. Die Sicherheit des Internet der Dinge bringt verschiedene Themen zusammen, d.h. Netzwerkprotokolle, Software, Hardware, Kryptographie und Cloud Computing.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte von IoT-Architekturen zu kennen und zu verstehen.
- die gängigsten Schwachstellen, Bedrohungen und Risiken für das Internet der Dinge zu kennen und zu verstehen.
- Gegenmaßnahmen für IoT-Schwachstellen zu verstehen und anzuwenden.
- ein IoT-Architekturmodell/eine IoT-Lösung zu analysieren.

Kursinhalt

1. Grundlagen des Internet der Dinge (IoT)
   - 1.1 Einführung
   - 1.2 Architektur
   - 1.3 Nicht-industrielles Internet der Dinge
   - 1.4 Industrie 4.0 (Industrielles IoT)
2. Angriffe auf das Internet der Dinge
   - 2.1 Verwundbarkeiten, Bedrohungen und Risiken
   - 2.2 Cyber-Angriffe und Gegenmaßnahmen
3. Sicherheit durch Design
   - 3.1 Projektmanagement / Sicherer Lebenszyklus der Entwicklung
   - 3.2 Statische Prüfung
   - 3.3 Dynamische Prüfung
   - 3.4 DevSecOps

4. Sichern von Geräten für das Internet der Dinge
   - 4.1 Sicherheitsrisiken
   - 4.2 Entwurfsziele
5. Operative Sicherheit
   - 5.1 Informations- und Cyber-Sicherheitsverwaltungssystem
   - 5.2 Netzwerk-Sicherheit
   - 5.3 Gerätekonfiguration
   - 5.4 Authentifizierung und Autorisierung
6. Cloud-Sicherheit
   - 6.1 Konzept des Nebels
   - 6.2 Bedrohungen für Cloud Internet of Things-Dienste
   - 6.3 Cloudbasierte Sicherheitsdienste
   - 6.4 Sichern der Cloud-Lösung
7. Big Data / Künstliche Intelligenz
   - 7.1 Beaufsichtigtes Lernen
   - 7.2 Unbeaufsichtigtes Lernen

Literatur

Pflichtliteratur

Weiterführende Literatur

- Butun, I. (2020): Industrial IoT. Challenges, Design Principles, Applications, and Security. 1st Edition, Springer International Publishing, Cham.
- Gupta B./Quamara, M. (2020): Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. 1st edition, CRC Press, Boca Raton, FL.
- Liyanage, M. et al. (2020): IoT Security. Advances in Authentication. 1st edition, John Wiley & Sons Ltd., Hoboken, NJ.
- Russell, B./Van Duren, D. (2018): Practical Internet of Things Security. Design a security framework for an Internet connected ecosystem. 2nd edition, Packt Publishing Ltd., Birmingham.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBCSEEIST01_D

Cyber Threat Intelligence

Module Code: DLBCSEECTI_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLBCSEECTI01_E	BA	10	300 h

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

Module Coordinator

N.N. (Attack Models and Threat Feeds) / N.N. (Project: Defense against APTs)

Contributing Courses to Module

- Attack Models and Threat Feeds (DLBCSEECTI01_E)
- Project: Defense against APTs (DLBCSEECTI02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Models and Threat Feeds • Study Format "Distance Learning": Exam, 90 Minutes Project: Defense against APTs • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Attack Models and Threat Feeds

- Apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model
- Determine what data is already available
- Do a gap analysis on what is detection or defense technology is missing
- Determine what extern threat feed data is required
- Utilize threat intelligence systems for diagnosis

Project: Defense against APTs

Using well-known methods like the MITRE ATT&CK Techniques, Tactics and Procedures students will be able to produce a comprehensive threat model. Therefore, students will have to determine through simulation or a “table top exercise” which data is already available and which extern threat feed data is required. After analyzing the “attack side” students will utilize threat intelligence systems for diagnostic to do a gap analysis – especially what defense technology is missing – and will be able to give sound advice to enhance resilience and to foster response capabilities. Emphasis will be drawn on the practical aspects of the defense against a given threat actor using techniques including beyond technical solutions and determine what cooperation with CERTs and ISPs is required to effectively defend against threats.

Learning Outcomes

Attack Models and Threat Feeds

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Project: Defense against APTs

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

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

Attack Models and Threat Feeds

Course Code: DLBCSEECTI01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, we look in depth at modeling threats and using data to diagnose, analyze and make recommendations. After a broad look at threat actors, we look at a variety of ways of modeling threats. This spans from Attack Trees to Kill Chains, but whichever method works the best, it all boils down to adversary Techniques, Tactics and Procedures. We look into the various taxonomies of these as defined by Mitre's ATT&CK and determine what can be observed in data.It is rare that internal data is enough for a complete analysis and in practice the threat analysist must use external data sources. These are available in a variety of formats, but the industry is converging on STIX and the use of software platforms like ACT to do the parsing and provide a good user experience.After looking at examples of threat actors and reports on them, we tackle the problem of making recommendations and writing reports. In some cases, engaging with law enforcement is required in which case some particularities need to be observed.

Course Outcomes

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Contents

1. Threat actors
   - 1.1 Script kiddies
   - 1.2 eCrime threat actors
   - 1.3 Advanced Persistent Threat actors (APT)
   - 1.4 Threat researchers

2. Modeling an attack
   - 2.1 Phases of an attack
   - 2.2 Lockheed Martin Kill-Chain
   - 2.3 Attack Trees
   - 2.4 STRIDE
   - 2.5 DREAD
   - 2.6 The Diamond Model of attack analysis
   - 2.7 Pyramid of pain
   - 2.8 Techniques, Tactics and Procedures

3. Attack preparation TTPs
   - 3.1 Observability of attack preparations
   - 3.2 Operational security of an organization

4. Enterprise TTPs
   - 4.1 Behaviors of the attacker
   - 4.2 Observable data in an enterprise

5. ICS TTPs
   - 5.1 Critical infrastructure
   - 5.2 Special considerations with IoT/ICS defense

6. Threat data exchange
   - 6.1 Indicators of Compromise
   - 6.2 Threat intelligence reports
   - 6.3 Ad-hoc data formats
   - 6.4 STIX format, TAXII protocol
   - 6.5 Mitre ATT&CK, CVEs, etc.
   - 6.6 The semantics of threat data
   - 6.7 Other sources of data for CTI analysis

7. Examples of threat analysis platforms
   - 7.1 ACT Platform
   - 7.2 MISP
   - 7.3 OpenCTI

8. Examples of threat actors and their modus operandi
   - 8.1 Threat model
   - 8.2 Relevant indicator data
   - 8.3 Relevant CTI data
   - 8.4 Diagnosing the threat
   - 8.5 Data coverage gap analysis

9. Reporting
   - 9.1 Mapping raw data to Mitre ATT&CK
   - 9.2 Making defensive recommendations
   - 9.3 Writing reports for technical staff
   - 9.4 Writing reports for management
   - 9.5 Working with law enforcement

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Defense against APTs

Course Code: DLBCSEECTI02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEECTI01_E

Course Description

This project course will give students hands-on experience in the challenging task to analyze threat vectors and real attacks of highly sophisticated, well planned, prepared and conducted attack campaigns named “Advanced Persistent Threats – APT´s” which derive from state, non-state or highly criminal attackers. Students will need to consider all practical aspects of different attack vectors using technical and non-technical (like social engineering) methods and procedures. To have the right understanding how to defend against these attacks they will use an attack simulator like Foreseeti SecureCAD or AttackIQ or conduct a “table top exercise” to figure out what data is required to analyze what security components and system configurations are needed to defend against a given, highly capable threat actor. Through this course, students will develop a complete overview what technical applications can be used to enhance resilience, foster response capabilities and recover from such attacks. Furthermore, students will have to take into account so called “soft measures” like organizational and procedural policies and regulations, bearing in mind the human factor in its social and psychological form. Through the cooperation with CERT´s, ISP´s and IT-Security Companies, academics and state agencies, students will cooperate on international level with IT-experts and experts from other disciplines to improve their expertise and to develop their personality.

Course Outcomes

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Contents

- This project course focuses on practical aspects how to defend against APTs. Students will start with a given use case to analyze a real-world APT Attack against a defined IT-System / Network, identify the different attack vectors on multiple levels and make the necessary data regarding used malware and exploits, techniques and procedures available by using a simulator or conducting a “table top exercise”. With this, students will develop a comprehensive picture of vulnerabilities and security shortfalls in the IT-system / network of

their own enterprise. Students will then have to analyze and identify what technical or non-technical measures could have prevented this attack using an interdisciplinary approach taking all levels and involved actors into account. Cooperation with other national and international CERT´s, ISP, IT-Security companies and state agencies will be the basis for a sound assessment how to improve the own resilience using best practices, state of the art technologies and considering new technologies.

- All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Telekommunikationspezifische Bedrohungen

Modulcode: DLBCSEEMT_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ keine ▪ DLBIBRVS01 oder DLBIBRVS01_E; DLBCSEINF01_D oder DLBCSEINF01_E	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Funk- und Telekommunikationssicherheit) / N.N. (Sofwarearchitektur mobiler Geräte)

Kurse im Modul

- Funk- und Telekommunikationssicherheit (DLBCSEEMT01_D)
- Sofwarearchitektur mobiler Geräte (DLBCSEEMT02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Funk- und Telekommunikationssicherheit • Studienformat "Fernstudium": Klausur, 90 Minuten Sofwarearchitektur mobiler Geräte • Studienformat "Fernstudium": Klausur, 90 Minuten

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Funk- und Telekommunikationssicherheit

- Überblick über drahtlose Protokolle
- Grundlagen von Drahtlosen Netwerken
- Telekommunikationsprotokoll-Klassen
- Telekom-Architektur
- Sicherheit von Handapparaten und Geräten
- Bedrohungen
- Andere drahtlose Anwendungen
- Schutzmaßnahmen

Sofwarearchitektur mobiler Geräte

- Mobil-Technologie-Stacks
- Hardware
- Android-Betriebssystem
- Apple iOS-Betriebssystem
- Mobile Geräte
- Software-Ökosysteme und Sicherheit
- Bedrohungen von Mobiltelefone
- Verwaltung mobiler Geräte

Qualifikationsziele des Moduls

Funk- und Telekommunikationssicherheit

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen der bei der Datenübertragung verwendeten drahtlosen Signale zu verstehen.
- verschiedene Arten der drahtlosen Vernetzung zu identifizieren und ihre Unterschiede zu verstehen.
- Telekommunikationsterminologie zu verstehen und diese der IT-Terminologie gegenüberzustellen.
- Architekturen der wichtigsten drahtlosen Telekommunikationssysteme zu verstehen.
- Angriffsvektoren gegen mobile Geräte sowie das Kernnetzwerk zu verstehen.
- andere Arten der Vernetzung, die möglicherweise genutzt werden, zu finden.

Sofwarearchitektur mobiler Geräte

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Hardware- und Software-Stacks gängiger Mobiltelefone zu verstehen.
- die Sicherheitskontrollen in diesen Stacks verstehen.
- zu erkennen, welche Schutzmaßnahmen und Risiken mit den Ökosystemen der Geräte verbunden sind.
- zu erkennen, welche Angriffe in der Vergangenheit erfolgreich waren.
- die Verwaltung mobiler Endgeräte zum Schutz eines Unternehmens zu nutzen.

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

Funk- und Telekommunikationssicherheit

Kurscode: DLBCSEEMT01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch	-1	5	DLBIBRVS01 oder DLBIBRVS01_E; DLBCSEINF01_D oder DLBCSEINF01_E

Beschreibung des Kurses

Die Zahl der Geräte, die drahtlos mit Netzwerken verbunden werden können, hat bereits die Zahl der Desktop- und Laptop-Computer überholt, die über ein Kabel mit einem lokalen Netzwerk verbunden sind. Vor allem Telefone und Tablets dominieren den Markt, die sich mit den drahtlosen Telekommunikationsnetzen verbinden. Es gibt aber auch viele andere Formen der drahtlosen Kommunikation, die von Geräten genutzt werden. Die Eigenheiten dieser drahtlosen Systeme müssen verstanden werden, um sie in ein vollständiges Sicherheitskonzept zu integrieren. Drahtlose Protokolle zwingen den User oft dazu, einem System zu vertrauen, in das er keinen Einblick hat. In diesem Kurs widmen wir uns genau diesem Thema.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen der bei der Datenübertragung verwendeten drahtlosen Signale zu verstehen.
- verschiedene Arten der drahtlosen Vernetzung zu identifizieren und ihre Unterschiede zu verstehen.
- Telekommunikationsterminologie zu verstehen und diese der IT-Terminologie gegenüberzustellen.
- Architekturen der wichtigsten drahtlosen Telekommunikationssysteme zu verstehen.
- Angriffsvektoren gegen mobile Geräte sowie das Kernnetzwerk zu verstehen.
- andere Arten der Vernetzung, die möglicherweise genutzt werden, zu finden.

Kursinhalt

1. Überblick über drahtlose Protokolle
   - 1.1 Netzwerkprotokolle für den persönlichen Bereich (Bluetooth, RFID, NFC und andere)
   - 1.2 Protokolle für drahtlose lokale Netzwerke (802.11a,b, g, ac , p und weitere)
   - 1.3 Wide Area Network-Protokolle (Telekommunikationsprotokolle, LoRa, Satellitenprotokolle und mehr)
   - 1.4 Schlüsselaustausch und Kryptographie in drahtlosen Netzwerken

2. Grundlagen von Drahtlosen Netwerken
   - 2.1 Frequenzen
   - 2.2 Modulationen
   - 2.3 Daten-Kodierungen
   - 2.4 Zielkonflikte

3. Telekommunikationsprotokoll-Klassen
   - 3.1 Telekommunikation vs. IT-Terminologie und -Technologien
   - 3.2 Telekommunikationsnormen
   - 3.3 Veraltete digitale Protokolle
   - 3.4 LTE
   - 3.5 5G

4. Telekom-Architektur
   - 4.1 Gesamtarchitektur
   - 4.2 Kern-Architektur
   - 4.3 Software-definierte Vernetzung
   - 4.4 5G-Campus-Netzwerke
   - 4.5 Sicherheit der Anwendungsschicht

5. Sicherheit von Handapparaten und Geräten
   - 5.1 Anforderungen
   - 5.2 Typischer Hardware-Entwurf
   - 5.3 IoT-Geräte

6. Bedrohungen
   - 6.1 Allgemeine Angriffsvektoren gegen (mobile) Geräte
   - 6.2 Allgemeine Angriffsvektoren gegen das Kernnetzwerk
   - 6.3 Mögliche Angriffe auf 5G-Campus-Netzwerke

7. Andere drahtlose Anwendungen
   - 7.1 Drahtlose Protokolle für Luftfahrt und Nautik
   - 7.2 Proprietäre Geräteprotokolle
   - 7.3 Großflächige Sensornetze (LoRa, Sigfox, ...)
   - 7.4 Digitale Sprach-/Datentechnologien (DECT/GAP, TETRA, ...)
   - 7.5 Satellitenkommunikation

8. Schutzmaßnahmen
   - 8.1 Mobile Technologie sicher integrieren
   - 8.2 Überwachung mobiler Geräte

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bartock, M. / Cichonski, J. / Souppaya, M. (2020): 5G CYBERSECURITY: Preparing a Secure Evolution to 5G.
- Cichonski, J. / Franklin, J. M. / Bartock, M. (2017): Guide to LTE Security. NIST Special Publication 800-187.
- Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/
- Pavur, J. et al. (2020): A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In 2020 IEEE Symposium on Security and Privacy (S&P). IEEE. May, 2020.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Sofwarearchitektur mobiler Geräte

Kurscode: DLBCSEEMT02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Mobile Geräte haben Desktops und Laptops als häufigste Endbenutzergeräte verdrängt. Das Smartphone ist zu einem zentralen Geschäftsinstrument geworden und User verwenden sie täglich für die unterschiedlichsten Anwendungen. Darüber hinaus nutzt auch das Internet der Dinge (IoT) diese mobilen Plattformen. Doch allzu oft sind die mit diesen mobilen Geräten verbundenen Risiken und Chancen insbesondere für die Sicherheitsadministratoren undurchsichtig, da diese Geräte oft außerhalb des traditionellen Intranets betrieben werden.In diesem Kurs untersuchen wir, wie die dominierenden Akteure, Android und Apple iOS, mit der Sicherheit in ihrem Softwarestack und ihrem Ökosystem umgehen. Wir betrachten auch das übersehene Problem der IoT-Sicherheit und schließen mit organisatorischen Lösungen ab.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Hardware- und Software-Stacks gängiger Mobiltelefone zu verstehen.
- die Sicherheitskontrollen in diesen Stacks verstehen.
- zu erkennen, welche Schutzmaßnahmen und Risiken mit den Ökosystemen der Geräte verbunden sind.
- zu erkennen, welche Angriffe in der Vergangenheit erfolgreich waren.
- die Verwaltung mobiler Endgeräte zum Schutz eines Unternehmens zu nutzen.

Kursinhalt

1. Mobil-Technologie-Stacks
   - 1.1 Hardware
   - 1.2 Firmware
   - 1.3 Betriebssystem
   - 1.4 Bewerbungen
   - 1.5 Ökosystem

2. Hardware
   - 2.1 RF-Module
   - 2.2 PDA-Modul
   - 2.3 Trusted Execution Environment
   - 2.4 Biometrische Geräte
   - 2.5 Standorttechnik

3. Android-Betriebssystem
   - 3.1 Hardware
   - 3.2 Bootloader
   - 3.3 Kernel- und Hardware-Abstraktionsschicht
   - 3.4 Sandboxing und Virtualisierung
   - 3.5 Code-Unterzeichnung

4. Apple iOS-Betriebssystem
   - 4.1 Hardware
   - 4.2 Bootloader
   - 4.3 Kernel und Frameworks
   - 4.4 Sandboxing und Virtualisierung
   - 4.5 Code-Unterzeichnung

5. Mobile Geräte
   - 5.1 Das Internet der Dinge
   - 5.2 Linux
   - 5.3 RTOS
   - 5.4 Android auf Geräten
   - 5.5 Andere gebräuchliche eingebettete Betriebssysteme

6. Software-Ökosysteme und Sicherheit
   - 6.1 Google Play
   - 6.2 Apple Store
   - 6.3 Sicherheitsanbieter
   - 6.4 Die Rolle der Cloud

7. Bedrohungen von Mobiltelefone
   - 7.1 Historische Beispiele für Angriffe auf Mobiltelefone
   - 7.2 Taxonomie der Bedrohungen von Mobiltelefonen
   - 7.3 Jailbreaking

8. Verwaltung mobiler Geräte
   - 8.1 Die Bedrohungen der BYOD
   - 8.2 Einzigartige Bedrohungen für mobile Geräte
   - 8.3 Verwaltung von Patches und Richtlinien

Literatur

Pflichtliteratur

Weiterführende Literatur

- Gupta, A. (2014): Learning Pentesting for Android Devices
- Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/
- N.A. (2020): Android Enterprise Security White Paper.
- N.A. (2019): iOS Security iOS 12.3. https://www.apple.com/lae/business/docs/site/iOS_Security_Guide.pdf
- Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

IT-Sicherheitsberatung

Modulcode: DLBCSEEISC_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ keine ▪ DLBCSEEISC01_D oder DLBCSEEISC01_E	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Technische und betriebliche IT-Sicherheitskonzeptionen (DLBCSEEISC01_D)
- Projekt: Einsatz und Konfiguration von SIEM-Systemen (DLBCSEEISC02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Technische und betriebliche IT-Sicherheitskonzeptionen • Studienformat "Fernstudium": Klausur, 90 Minuten Projekt: Einsatz und Konfiguration von SIEM-Systemen • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Technische und betriebliche IT-Sicherheitskonzeptionen

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

Projekt: Einsatz und Konfiguration von SIEM-Systemen

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

Qualifikationsziele des Moduls

Technische und betriebliche IT-Sicherheitskonzeptionen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Projekt: Einsatz und Konfiguration von SIEM-Systemen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Technische und betriebliche IT-Sicherheitskonzeptionen

Kurscode: DLBCSEEISC01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

2. Schutz-Profile
   - 2.1 Referenzarchitektur, Technologie und Netzwerkbetrieb
   - 2.2 Risikobewertung, Restrisiko und Risikomanagement
   - 2.3 Sicherheitsanforderungen und Schutzmaßnahmen
   - 2.4 Sicherheitsbewertung von IT-Sicherheitsprodukten
   - 2.5 Akkreditierung von IT-Systemen und Netzwerken

3. Systeme der Intrusion Detection
   - 3.1 Erkennungsstrategie,
   - 3.2 Datenquellen, Sensoren
   - 3.3 Analytik
   - 3.4 Indikatoren für Kompromittierungen

4. Netzwerk-Überwachung
   - 4.1 Systeme zum Schutz vor Bedrohungen
   - 4.2 Technologie drahtloser Sensornetzwerke
   - 4.3 Austausch von Bedrohungsinformationen

5. Sicherheitsinformationen und Ereignismanagement (SIEM)
   - 5.1 Technische und betriebliche Daten-Quellen
   - 5.2 DATA-Fusion
   - 5.3 Normverhalten von Netzwerken
   - 5.4 Analyse großer Datenmengen - Übertragung technischer Daten in operative Informationen
   - 5.5 IT- Sicherheitslage und Lagebewusstsein
   - 5.6 Strategien zur Reaktion auf Vorfälle und automatisierte Gegenmaßnahmen

6. IT-Sicherheitsevaluierung und -bewertung
   - 6.1 IT-Sicherheits-Metriken
   - 6.2 Bewertung der IT-Sicherheit

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt: Einsatz und Konfiguration von SIEM-Systemen

Kurscode: DLBCSEEISC02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSEEISC01_D oder DLBCSEEISC01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Social Engineering

Modulcode: DLBCSEESE_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ DLBCSEESE01_D oder DLBCSEESE01_E ▪ keine	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Social Engineering und Insider Threats (DLBCSEESE01_D)
- Projekt: Social Engineering (DLBCSEESE02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Social Engineering und Insider Threats • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Fallstudie Projekt: Social Engineering • Studienformat "Fernstudium": Projektpräsentation

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Social Engineering und Insider Threats

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

Projekt: Social Engineering

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

Qualifikationsziele des Moduls

Social Engineering und Insider Threats

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Projekt: Social Engineering

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Social Engineering und Insider Threats

Kurscode: DLBCSEESE01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

1. Methoden des Social Engineering
   - 1.1 Phishing, Speer-Phishing
   - 1.2 Quid pro quo, Köder, Medienabwurf
   - 1.3 Scareware, CEO-Betrug
   - 1.4 Vorwände, Heckenschützen

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

3. Erkennung von Insider-Bedrohungen
   - 3.1 DATA Mining zur Erkennung von Insider-Bedrohungen,
   - 3.2 Umfassender Rahmen für die Aufdeckung und Reaktion auf Insider-Bedrohungen
   - 3.3 Werkzeuge zur Selbsteinschätzung für die Evaluierung,
   - 3.4 Organisatorisches Lernen
   - 3.5 Innovative Prozesse
   - 3.6 Anwendung von Methoden des maschinellen Lernens

4. Sicherheitspolitik und -vorschriften
   - 4.1 Organisatorischer Rahmen, Compliance, Verhaltenskodex
   - 4.2 Ausbildung
   - 4.3 System zur Reaktion auf Zwischenfälle
   - 4.4 Schutz von klassifizierten / sensiblen Informationen
   - 4.5 Passwort-Richtlinie
   - 4.6 Datenspeicherung und Zugriffsprofile
   - 4.7 Schnittstellenüberwachung und -regulierung (USB-Politik, ...)

5. Nationale und internationale Zusammenarbeit und Informationsaustausch.
   - 5.1 Zusammenarbeit mit Internet Service Providern (ISP) und Interessenvertretern der IT-Sicherheit
   - 5.2 Austauschplattformen und Foren für taktische Techniken und Verfahren (TTP's) und bewährte Praktiken
   - 5.3 Zusammenarbeit mit nationalen Sicherheitsbehörden

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Fallstudie

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

Projekt: Social Engineering

Kurscode: DLBCSEESE02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBCSEESE01_D oder DLBCSEESE01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Projektpräsentation

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Host Forensics

Module Code: DLBCSEEHF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEHSF01_E or DLBCSEHSF01_D ▪ DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E	BA	10	300 h

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

Module Coordinator

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

Contributing Courses to Module

- Static and Dynamic Malware Analysis (DLBCSEEHF01_E)
- Seminar: Sandbox Interpretation (DLBCSEEHF02_E)

Module Exam Type

Module Exam	Split Exam
	Static and Dynamic Malware Analysis • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Sandbox Interpretation • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Static and Dynamic Malware Analysis

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

Seminar: Sandbox Interpretation

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

Learning Outcomes

Static and Dynamic Malware Analysis

On successful completion, students will be able to

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

Seminar: Sandbox Interpretation

On successful completion, students will be able to

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

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

Static and Dynamic Malware Analysis

Course Code: DLBCSEEHF01_E

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

Course Description

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

Course Outcomes

On successful completion, students will be able to

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

Contents

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

4. Malware Classification
   - 4.1 Antivirus
   - 4.2 Virustotal
   - 4.3 Yara
   - 4.4 Clustering with PEID, TELFHASH, TLSH, SSDEEP, etc

5. Sandboxes
   - 5.1 Levels of interaction
   - 5.2 Instrumentation
   - 5.3 Online sandboxing services, Virustotal
   - 5.4 Scripting for sandboxes
   - 5.5 Corporate sandbox considerations

6. Reversing
   - 6.1 Unpacking, decrypting and de-obfuscation
   - 6.2 Debugging techniques
   - 6.3 Control flow analysis
   - 6.4 Library and system calls

7. Digging deeper
   - 7.1 Domain and IP information
   - 7.2 Analysis of Javascript code
   - 7.3 Memory forensics
   - 7.4 Kernel debugging rootkits
   - 7.5 Theoretical underpinnings of program analysis

Literature

Compulsory Reading

Further Reading

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

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Sandbox Interpretation

Course Code: DLBCSEEHF02_E

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

Course Description

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

Course Outcomes

On successful completion, students will be able to

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

Contents

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

Literature

Compulsory Reading

Further Reading

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

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBCSEEHF02_E

DevSecOps

Modulcode: DLBCSEEDSO_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ IWNF01 oder IWNF01_E ▪ keine	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

- Techniken und Methoden der agilen Softwareentwicklung (IWNF01)
- Projekt: Agiles DevSecOps-Software-Engineering (DLBCSEEDSO01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Techniken und Methoden der agilen Softwareentwicklung • Studienformat "Fernstudium": Klausur, 90 Minuten Projekt: Agiles DevSecOps-Software-Engineering • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Techniken und Methoden der agilen Softwareentwicklung

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

Projekt: Agiles DevSecOps-Software-Engineering

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

Qualifikationsziele des Moduls

Techniken und Methoden der agilen Softwareentwicklung

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Projekt: Agiles DevSecOps-Software-Engineering

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

Techniken und Methoden der agilen Softwareentwicklung

Kurscode: IWNF01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Agiles Portfolio- und Projektmanagement
   - 3.1 Planungsebenen im agilen Projektmanagement
   - 3.2 Agiles Portfoliomanagement
   - 3.3 Organisation mehrerer Teams in einem Projekt
   - 3.4 Produkt- und Release-Planung

4. Agiles Anforderungs- und IT-Architekturmanagement
   - 4.1 Requirements Engineering in agilen Projekten
   - 4.2 Architekturmanagement in agilen Projekten

5. Agiles Testen
   - 5.1 Grundlagen und Anforderungen an die QS-Organisation
   - 5.2 Teststufen und Agilität
   - 5.3 Testautomatisierung

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt: Agiles DevSecOps-Software-Engineering

Kurscode: DLBCSEEDSO01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IWNF01 oder IWNF01_E

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

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

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLBCSEEDSO01_D

Sicherheit in komplexen Netzwerken

Modulcode: DLBCSEESCN_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	IAMG01 oder DLBCSEITPAM02	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Tobias Brückmann (IT-Architekturmanagement) / N.N. (Projekt: IT-Sicherheitsarchitekturen)

Kurse im Modul

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

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	IT-Architekturmanagement • Studienformat "Fernstudium": Klausur, 90 Minuten Projekt: IT-Sicherheitsarchitekturen • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

IT-Architekturmanagement

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

Projekt: IT-Sicherheitsarchitekturen

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

Qualifikationsziele des Moduls

IT-Architekturmanagement

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Projekt: IT-Sicherheitsarchitekturen

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

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

IT-Architekturmanagement

Kurscode: IAMG01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

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

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

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

3. Architektur-Governance
   - 3.1 Aufbauorganisation
   - 3.2 Entwicklung und Durchsetzung von Richtlinien
   - 3.3 Projektbegleitung

4. Modellierung von IT-Unternehmensarchitekturen
   - 4.1 Modelle im Kontext IT-Architekturmanagement
   - 4.2 Dokumentationsformen für Prozesse und Anwendungen
   - 4.3 Dokumentationsformen für Systeme und Technologien

5. Frameworks am Beispiel von TOGAF
   - 5.1 Grundlagen und Einsatz von IT-Architekturframeworks
   - 5.2 Überblick und Kategorien von EAM-Frameworks
   - 5.3 The Open Group Architecture Framework (TOGAF)

6. Referenzmodelle und Musterkataloge
   - 6.1 Referenzmodelle für Architekturen
   - 6.2 Musterkatalog für Gestaltung von EAM

Literatur

Pflichtliteratur

Weiterführende Literatur

- Hanschke, I. (2011): Enterprise Architecture Management. Einfach und effektiv. Hanser, München.
- Keller, W. (2012): IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung. 2. Auflage, dpunkt.verlag, Heidelberg.
- Keuntje. J. H./Barkow, R. (Hrsg.) (2010): Enterprise Architecture. Management in der Praxis. Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen.
- Ross, J. W./ Weill, P./Robertson, D. C. (2006): Enterprise Architecture as Strategy. Creating a Foundation for Business Execution. Harvard Business Review Press, Boston.
- Schwarzer, B. (2009): Einführung in das Enterprise Architecture Management. Verstehen – Planen – Umsetzen. Books on Demand, Norderstedt.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Projekt: IT-Sicherheitsarchitekturen

Kurscode: DLBCSEESCN01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IAMG01 oder DLBCSEITPAM02

Beschreibung des Kurses

Unter Verwendung von Methoden und Techniken aus dem Bereich IT-Architekturmanagement bearbeiten die Studierenden in diesem Kurs selbständig eine praktische Fragestellung im Bereich der IT-Sicherheitsarchitektur. Am Ende des Kurses sind die Studierenden in der Lage, auf der Basis einer bestehenden IT-System- / Netzwerkarchitektur eine IT-Sicherheitsarchitektur selbstständig zu entwickeln.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

- Umsetzung und Dokumentation praktischer Fragen zur IT-Sicherheit im Rahmen des IT-Architekturmanagements. Typische Szenarien sind z.B. "Implementierung von IT-Sicherheitsgeräten in komplexen Netzwerken", "Gestaltung von Prozessen für Sicherheitsupdates und Patch-Management" und "Einsatz von Inhouse-Ressourcen oder Outsourcing von IT-Sicherheitsaufgaben".

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Bartsch, M. / Frey, S. (2014): Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Fachmedien, Wiesbaden. ▪ Müller, K.-R. (2014): IT-Sicherheit mit System. 5. Auflage, Springer Fachmedien, Wiesbaden. ▪ Pfister, M. (2019): Info Guard Swiss Cyber Security - In 3 einfachen (aber wichtigen) Schritten zur Enterprise IT-Sicherheitsarchitektur. (URL: www.infoguard.ch [zuletzt besucht am 22.08.2020]).

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Network Forensics

Module Code: DLBCSEENF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E ▪ DLBCSEINF01_E or DLBCSEINF01_D	BA	10	300 h

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

Module Coordinator

N.N. (Protocols, Log- and Dataflow-Analysis in Depth) / N.N. (Seminar: Threat Hunting, Analysis and Incident Response)

Contributing Courses to Module

- Protocols, Log- and Dataflow-Analysis in Depth (DLBCSEENF01_E)
- Seminar: Threat Hunting, Analysis and Incident Response (DLBCSEENF02_E)

Module Exam Type

Module Exam	Split Exam
	Protocols, Log- and Dataflow-Analysis in Depth • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Threat Hunting, Analysis and Incident Response • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Protocols, Log- and Dataflow-Analysis in Depth

- Introduction
- Basic protocol layering
- Operating system logs
- HTTP server
- IP Firewall
- Web application filter
- Authentication servers
- Databases
- Intrusion Detection and Protection System (IDPS)
- Email systems
- Content filters
- SSH
- Less common systems
- Context
- Log management Infrastructure
- Security Information and Event Management (SIEM)
- Visualization
- Security Operations Centers (SOC)
- Logging in the cloud
- Dataflow monitoring
- Attacks against logging
- Analysis techniques
- Reporting

Seminar: Threat Hunting, Analysis and Incident Response

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

Learning Outcomes

Protocols, Log- and Dataflow-Analysis in Depth

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Seminar: Threat Hunting, Analysis and Incident Response

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

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

Protocols, Log- and Dataflow-Analysis in Depth

Course Code: DLBCSEENF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D

Course Description

Logging is done for a variety of diagnosis reasons, but these logs can be very useful in finding security incidents. In this course, we look at a variety of sources of log files. These range from operating system logs, to application logs and network traffic logs. Context and additional information also need to be collected. All this data is then consolidated in a Security Information and Event Management system where it can be analyzed and triaged for action. Finally, major incidents need to be documented and communicated to the relevant parties.

Course Outcomes

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Contents

1. Introduction
   - 1.1 Network protocols
   - 1.2 Applications of log files
   - 1.3 Operating system log files
   - 1.4 Application log files
   - 1.5 Network log files
   - 1.6 Dataflow logs
   - 1.7 Security log files

2. Basic protocol layering
   - 2.1 Internet protocol hierarchy
   - 2.2 TCP connection
   - 2.3 Frame layer
   - 2.4 Ethernet layer
   - 2.5 Internet Protocol layer
   - 2.6 Transport Control Protocol
   - 2.7 UDP packets
   - 2.8 TCP/IP in relation to the OSI layer model
   - 2.9 Reading RFCs and related documentation
3. Operating system logs
   - 3.1 Syslog
   - 3.2 System events
   - 3.3 Audit events
4. HTTP server
   - 4.1 Common server vendors
   - 4.2 Apache log format
   - 4.3 Web edge logging
   - 4.4 Logs from Content delivery networks
5. IP Firewall
6. Web application filter
7. Authentication servers
8. Databases
9. Intrusion Detection and Protection System (IDPS)
10. Email systems
    - 10.1 SMTP
    - 10.2 POP
    - 10.3 Exchange

11. Content filters
    - 11.1 Spam and Phish filters
    - 11.2 Malware filters
    - 11.3 Data leak prevention
12. SSH
13. Less common systems
    - 13.1 MQTT
    - 13.2 CoAP
    - 13.3 XMPP
    - 13.4 BGP
    - 13.5 RIP
    - 13.6 DNS
14. Context
    - 14.1 Asset management
    - 14.2 Known vulnerable systems
    - 14.3 Network topology
15. Log management Infrastructure
    - 15.1 Log generation
    - 15.2 Storage
    - 15.3 Analysis
    - 15.4 Monitoring
    - 15.5 Security and privacy of logs
    - 15.6 Roles and responsibility
    - 15.7 Policies
    - 15.8 Long term log storage
16. Security Information and Event Management (SIEM)
17. Visualization
18. Security Operations Centers (SOC)
19. Logging in the cloud
20. Dataflow monitoring

21. Attacks against logging

22. Analysis techniques
    - 22.1 Entry Normalization
    - 22.2 Semantics of log events
    - 22.3 Prioritizing entries
    - 22.4 Aggregation
    - 22.5 Rule based systems
    - 22.6 Anomaly detection
    - 22.7 Machine learning
    - 22.8 Triaging incidents
    - 22.9 Working with filters

23. Reporting
    - 23.1 Indicators of compromise
    - 23.2 Mapping to the Mitre ATT&CK framework
    - 23.3 STIX, TAXII
    - 23.4 Written reports and presentations

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- NIST Special Publicaton 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Threat Hunting, Analysis and Incident Response

Course Code: DLBCSEENF02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E

Course Description

Much of a security officer's work is with data where incidents need to be analyzed and countermeasures implemented. This course uses the Mitre ATT&CK® framework to reference TTPs (Techniques, Tactics and Procedures) that map to security events. Not all TTPs can be found in labeled security events, so Threat Hunting aims to go beyond ordinary incident response and find indicators of these TTPs also using other methods.

Course Outcomes

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Contents

- In this seminar, we cover the subjects of incident response and threat hunting using the Mitre ATT&CK® framework and publicly available reports.

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Business Intelligence

Modulcode: IWBI

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Dr. Peter Poensgen (Business Intelligence) / Dr. Peter Poensgen (Projekt Business Intelligence)

Kurse im Modul

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

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Business Intelligence • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "Kombistudium": Klausur, 90 Minuten Projekt Business Intelligence • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Business Intelligence

- Motivation und Begriffsbildung
- Datenbereitstellung
- Data Warehouse
- Modellierung multidimensionaler Datenräume
- Analysesysteme
- Distribution und Zugriff

Projekt Business Intelligence

Mögliche Themengebiete für das BI-Projekt sind u.a. „Management von BI-Projekten, „Konzeption von multidimensionalen Datenmodellen“ sowie „Prototypische Umsetzung von kleinen BI-Anwendungen“.

Qualifikationsziele des Moduls

Business Intelligence

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivation, Anwendungsfälle und Grundlagen für Business Intelligence zu erklären.
- Techniken und Methoden zur Bereitstellung und Modellierung von Daten sowie für BI relevante Arten von Daten zu benennen und zu erläutern sowie voneinander abzugrenzen.
- Techniken und Methoden zur Informationsgenerierung und -speicherung zu erläutern und auf Basis konkreter Anforderungen selbstständig geeignete Methoden auszuwählen.

Projekt Business Intelligence

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine Lösung zu einer praktischen Fragestellung im Thema Business Intelligence zu konzipieren, prototypisch umzusetzen und die dabei erzielten Ergebnisse zu dokumentieren.
- typische Probleme und Herausforderungen in der Konzeption und praktischen Umsetzung kleiner BI-Lösungen zu benennen und zu erläutern.

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

Business Intelligence

Kurscode: IWBI01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Business Intelligence (BI) dient der Gewinnung von Informationen aus Unternehmensdaten, die sowohl für eine gezielte Unternehmenssteuerung als auch für die Optimierung von Geschäftsaktivitäten relevant sind. Im Rahmen dieses Kurses werden Techniken, Vorgehensweisen und Modelle zur Datenbereitstellung, Informationsgenerierung und -analyse sowie der Verteilung der gewonnenen Informationen vorgestellt und diskutiert. Sie werden danach in der Lage sein, die verschiedenen Themengebiete des Data Warehousing zu erläutern und Methoden bzw. Techniken für konkrete Anforderungen selbstständig auszuwählen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Motivation, Anwendungsfälle und Grundlagen für Business Intelligence zu erklären.
- Techniken und Methoden zur Bereitstellung und Modellierung von Daten sowie für BI relevante Arten von Daten zu benennen und zu erläutern sowie voneinander abzugrenzen.
- Techniken und Methoden zur Informationsgenerierung und -speicherung zu erläutern und auf Basis konkreter Anforderungen selbstständig geeignete Methoden auszuwählen.

Kursinhalt

1. Motivation und Begriffsbildung
   - 1.1 Motivation und historische Entwicklung
   - 1.2 BI als Rahmenwerk
2. Datenbereitstellung
   - 2.1 Operative und dispositive Systeme
   - 2.2 Das Data-Warehouse-Konzept
   - 2.3 Architekturvarianten
3. Data Warehouse
   - 3.1 ETL-Prozess
   - 3.2 DWH und Data Mart
   - 3.3 ODS und Metadaten

4. Modellierung multidimensionaler Datenräume
   - 4.1 Datenmodellierung
   - 4.2 OLAP-Würfel
   - 4.3 Physische Speicherung
   - 4.4 Star- und Snowflake-Schema
   - 4.5 Historisierung

5. Analysesysteme
   - 5.1 Freie Datenrecherche und OLAP
   - 5.2 Berichtssysteme
   - 5.3 Modellgestützte Analysesysteme
   - 5.4 Konzeptorientierte Systeme

6. Distribution und Zugriff
   - 6.1 Informationsdistribution
   - 6.2 Informationszugriff

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bachmann, R./Kemper, G. (2011): Raus aus der BI-Falle. Wie Business Intelligence zum Erfolg wird. 2. Auflage, mitp, Heidelberg.
- Bauer, A./Günzel, H. (2008): Data Warehouse Systeme. Architektur, Entwicklung, Anwendung. 3. Auflage, dpunkt.verlag, Heidelberg.
- Betz, R. (2015): Werde Jäger des verlorenen Schatzes. In: Immobilienwirtschaft, Heft 5, S. 1614–1164. (URL https://www.haufe.de/download/immobilienwirtschaft-ausgabe-052015-immobilienwirtschaft-fachmagazin-fuer-management-recht-praxis-303530.pdf [letzter Zugriff: 27.02.2017]).
- Bodendorf, F. (2006): Daten- und Wissensmanagement. 2. Auflage, Springer, Berlin.
- Chamoni, P./Gluchowski, P. (Hrsg.) (2006): Analytische Informationssysteme Business Intelligence-Technologien und -Anwendungen. Springer, Berlin.
- Engels, C. (2008): Basiswissen Business Intelligence. W3L, Herdecke/Witten.
- Gansor, T./Totok, A./Stock, S. (2010): Von der Strategie zum Business Intelligence Competency Center (BICC). Konzeption – Betrieb – Praxis. Hanser, München.
- Gluchowski, P./Gabriel, R./Dittmar, C. (2008): Management Support Systeme und Business Intelligence. Computergestützte Informationssysteme für Fach- und Führungskräfte. 2. Auflage, Springer, Berlin/Heidelberg.
- Grothe, M. (2000): Business Intelligence. Aus Informationen Wettbewerbsvorteile gewinnen. Addison-Wesley, München.
- Gutenberg, E. (1983): Grundlagen der Betriebswirtschaft, Band 1. Die Produktion. 18. Auflage, Springer, Berlin/Heidelberg/New York.
- Hannig, U. (Hrsg.) (2002): Knowledge Management und Business Intelligence. Springer, Berlin.
- Hansen, H.-R./Neumann, G. (2001): Wirtschaftsinformatik I. Grundlagen betrieblicher Informationsverarbeitung. 8. Auflage, Lucius & Lucius UTB, Stuttgart.
- Humm, B./Wietek, F. (2005): Architektur von Data Warehouses und Business Intelligence Systemen. In: Informatik Spektrum, S. 3–14. (URL: https://www.fbi.h-da.de/fileadmin/personal/b.humm/Publikationen/Humm__Wietek_-_Architektur_DW__Informatik-Spektrum_2005-01_.pdf [letzter Zugriff: 27.02.2017]).
- Kemper, H.-G./Baars, H./Mehanna, W. (2010): Business Intelligence – Grundlagen und praktische Anwendungen. Eine Einführung in die IT-basierte Managementunterstützung. 3. Auflage, Vieweg+Teubner, Stuttgart.
- Turban, E. et al. (2010): Business Intelligence. A Managerial Approach. 2. Auflage, Prentice Hall, Upper Saddle River (NJ).

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☐ Live Tutorium/Course Feed

Projekt Business Intelligence

Kurscode: IWBI02

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Unter Anwendung bekannter Methoden und Techniken aus dem Themengebiet Business Intelligence bearbeiten die Studierenden in diesem Kurs selbstständig eine praktische Fragestellung.Zum Abschluss des Kurses können Sie selbstständig auf der Grundlage konkreter Anforderungen Business Intelligence-Anwendungen konzipieren und prototypisch umsetzen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine Lösung zu einer praktischen Fragestellung im Thema Business Intelligence zu konzipieren, prototypisch umzusetzen und die dabei erzielten Ergebnisse zu dokumentieren.
- typische Probleme und Herausforderungen in der Konzeption und praktischen Umsetzung kleiner BI-Lösungen zu benennen und zu erläutern.

Kursinhalt

- Umsetzung und Dokumentation von praktischen Fragestellungen zum Einsatz von Business Intelligence-Anwendungen. Typische Szenarien sind beispielsweise „Management von BI-Projekten“, „Konzeption von multidimensionalen Datenmodellen“ und „Prototypische Umsetzung von kleinen BI-Anwendungen“.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Brenner, W./Uebernickel, F. (2015): Design Thinking. Das Handbuch. Frankfurter Allgemeine Buch, Frankfurt a. M.
- Brown, T. (2008): Design Thinking. In: Harvard Business Review, Heft Juni, S. 84–95.
- Meinel, C./Weinberg, U./Krohn, T. (Hrsg.) (2015): Design Thinking Live. Wie man Ideen entwickelt und Probleme löst. Murmann, Hamburg.
- Uebernickel, F./Brenner, W. (2016): Design Thinking. In: Hoffmann, C. P. et al. (Hrsg.): Business Innovation: Das St. Galler Modell. Springer, Wiesbaden, S. 243–265.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden

- ☐ Learning Sprints®
- ☐ Skript
- ☐ Vodcast
- ☐ Shortcast
- ☐ Audio
- ☐ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☑ Prüfungsleitfaden
- ☐ Live Tutorium/Course Feed

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Future Threats

Modulcode: DLBCSEEFT_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ IREN01 oder DLBCSRE01; DLBCSEEFT01_D oder DLBCSEEFT01_E ▪ IREN01 oder DLBCSRE01	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Threat Modeling) / N.N. (Projekt: Threat Modeling)

Kurse im Modul

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

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Threat Modeling

- C.I.A. Denken und mehr
- Messung der Cyber-Bedrohung
- Modellierung von Bedrohungen
- Bibliotheken angreifen
- Regeln, Vorschriften und Strafverfolgung
- Risiko-Management
- Threat Mitigation

Projekt: Threat Modeling

Dieser Kurs behandelt die Theorie und Praxis des Auffindens und der Modellierung von Bedrohungen in einem bestimmten System, einer bestimmten Architektur oder einem bestimmten Szenario. Er behandelt Methoden und Quellen für übliche Bedrohungsmuster. In einem Projekt wird die Theorie in die Praxis umgesetzt, indem eine gegebene Situation auf Bedrohungen analysiert wird.

Qualifikationsziele des Moduls

Threat Modeling

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- souverän mögliche Bedrohungsarten zu durchdenken.
- diese Bedrohungen mit Hilfe einer gebräuchlichen Modellierungsmethode zu modellieren.
- relevante Techniken, Taktiken und Verfahren in Bezug auf ein bestimmtes Szenario zu finden.
- das aus dem Bedrohungsmodell hervorgehende Risiko zu ermitteln.
- das Risiko durch die Implementierung von Änderungen des Designs zu mindern.

Projekt: Threat Modeling

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihr Wissen über die Modellierung von Bedrohungen auf Fälle und Szenarien anzuwenden.
- ihr daraus resultierendes Modell auf der Grundlage einer soliden Argumentation und in Bezug auf bekannte Techniken, Taktiken und Verfahren der Angreifer zu rechtfertigen.
- einen Bericht zu verfassen, der ihre Argumentation in systematischer und verständlicher Weise darlegt.

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

Threat Modeling

Kurscode: DLBCSEEFT01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01

Beschreibung des Kurses

Wenn ein System oder eine Architektur geschaffen wird, ist es wichtig, dass mögliche Bedrohungen gleichzeitig bewertet werden. Durch die Verwendung sowohl von Modellierungsmethoden als auch von in der Vergangenheit beobachteten Angriffsmustern ist es möglich, ein neues oder bestehendes System auf Bedrohungen hin zu untersuchen. Aus dieser Analyse lassen sich Risiken und Maßnahmen zu deren Verminderung ableiten. Während die gebräuchlichsten Methoden auf den Angriffsbäumen und dem STRIDE-Modell basieren, werden bei der Angriffsmodellierung in letzter Zeit auch Repositorien von Angreifer-Techniken, -Taktiken und -Verfahren (TTP´s) zur Inspiration herangezogen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- souverän mögliche Bedrohungsarten zu durchdenken.
- diese Bedrohungen mit Hilfe einer gebräuchlichen Modellierungsmethode zu modellieren.
- relevante Techniken, Taktiken und Verfahren in Bezug auf ein bestimmtes Szenario zu finden.
- das aus dem Bedrohungsmodell hervorgehende Risiko zu ermitteln.
- das Risiko durch die Implementierung von Änderungen des Designs zu mindern.

Kursinhalt

1. C.I.A. Denken und mehr
   - 1.1 Vertraulichkeit (Confidentiality)
   - 1.2 Integrität (Integrity)
   - 1.3 Verfügbarkeit (Availability)
   - 1.4 Sicherheit und andere Belange
2. Messung der Cyber-Bedrohung
   - 2.1 Messung und Verwaltung
   - 2.2 Metriken zur Cyber-Bedrohung
   - 2.3 Messung der Bedrohung für eine Organisation
   - 2.4 Die Wahrscheinlichkeit größerer Cyber-Angriffe
   - 2.5 Black Swan events

3. Modellierung von Bedrohungen
   - 3.1 Methodik des Angrifssbaumes
   - 3.2 STRIDE
   - 3.3 DREAD
   - 3.4 Schmerzpyramide – “Pyramid of Pain”

4. Bibliotheken angreifen
   - 4.1 CAPEC
   - 4.2 Soloves Taxonomie der Privatsphäre
   - 4.3 Modellierung mit Mitre ATT&CK®
   - 4.4 Identifizierung neuer Arten von Angriffen

5. Regeln, Vorschriften und Strafverfolgung
   - 5.1 Cyber-Gesetze
   - 5.2 Compliance und Strafverfolgung

6. Risiko-Management
   - 6.1 Veränderte Herangehensweisen an das Risikomanagement
   - 6.2 Reaktion auf Zwischenfälle und Krisenmanagement
   - 6.3 Berücksichtigung der Black Swan Events
   - 6.4 Kontinuierliche Neubewertung

7. Threat Mitigation
   - 7.1 Defensive Taktiken und Technologien
   - 7.2 Strategien zur Risikominderung
   - 7.3 Validierung des Abwehrschutzes
   - 7.4 Sicherheit und Privacy by Design
   - 7.5 Implementierung von Mechanismen zur Verminderung der Bedrohungen in einer Organisation

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ CAPEC: Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/ ▪ Kim, P. (2014): The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2015): The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2018): The Hacker Playbook 3: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Mitre ATT&CK®. https://attack.mitre.org/ ▪ Pfleeger, C. P. / Pfleeger, S. L. / Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London. ▪ Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☑ Vodcast	☐ Prüfungsleitfaden
☐ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt: Threat Modeling

Kurscode: DLBCSEEFT02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	IREN01 oder DLBCSRE01; DLBCSEEFT01_D oder DLBCSEEFT01_E

Beschreibung des Kurses

Die Bedrohungen für moderne Computersysteme sind vielfältig und entwickeln sich ständig weiter. In diesem Projekt hat der Studierende die Gelegenheit, die Kunst und Wissenschaft der Bedrohungsmodellierung auf ein Szenario anzuwenden, das vom Dozenten zusammen mit dem Studierenden definiert wird. Die Grundlage bilden reale oder fiktive Fallstudien, zu denen der Studierende unter Verwendung einer geeigneten Methodik die Bedrohungen identifizieren und darüber berichten soll. Diese kann aus Methoden wie Attack Trees, STRIDE, DREAD oder einer gerechtfertigten Aufzählung von CAPEC oder Mitre ATT&CK® TTPs ausgewählt werden, je nachdem, was der Kursteilnehmer für am geeignetsten hält. Die Ergebnisse werden in Form eines Berichts präsentiert.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ihr Wissen über die Modellierung von Bedrohungen auf Fälle und Szenarien anzuwenden.
- ihr daraus resultierendes Modell auf der Grundlage einer soliden Argumentation und in Bezug auf bekannte Techniken, Taktiken und Verfahren der Angreifer zu rechtfertigen.
- einen Bericht zu verfassen, der ihre Argumentation in systematischer und verständlicher Weise darlegt.

Kursinhalt

- Für einen bestimmten Fall oder ein bestimmtes Szenario modellieren Studierende die Bedrohungen unter Verwendung einer etablierten Methodik und reicht dann den Bericht und, falls zutreffend, alle Codes und Daten ein. Spezifische Probleme und Kontexte werden vom Tutor vorgegeben, Vorschläge der Studierenden können jedoch berücksichtigt werden.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Case Studies (Cyber): https://www.securitymagazine.com/topics/2664-case-studies-cyber ▪ Karger, P. A. / Scherr, R. R. (1974): MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS. ▪ Palmer, C. C. (2001): Ethical Hacking.IBM Systems Journal. 40 (3):769. ▪ Shostack, A. 2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ. ▪ Van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLBCSEEFT02_D

Cloud Security

Module Code: DLBCSEECS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBDSCC01 or DLBDSCC01_D ▪ DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E	BA	10	300 h

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

Module Coordinator

N.N. (Security Controls in the Cloud) / N.N. (Project: Security by Design in the Cloud)

Contributing Courses to Module

- Security Controls in the Cloud (DLBCSEECS01_E)
- Project: Security by Design in the Cloud (DLBCSEECS02_E)

Module Exam Type

Module Exam	Split Exam
	Security Controls in the Cloud • Study Format "Distance Learning": Exam, 90 Minutes Project: Security by Design in the Cloud • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Security Controls in the Cloud

- Cloud security
- Losing the intranet
- Security by design
- Secure cloud coding
- Confidentiality aspects
- Monitoring and Audit

Project: Security by Design in the Cloud

This module is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Learning Outcomes

Security Controls in the Cloud

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Project: Security by Design in the Cloud

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

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

Security Controls in the Cloud

Course Code: DLBCSEECS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D

Course Description

Maintaining a datacenter is expensive and inflexible, so it is expected that most corporations will be moving their server-based processes to a private, public or hybrid cloud in the next few years. Doing so will make operations more flexible and elastic but poses challenges to security architectures and operations. The paradigm of Infrastructure as Code (IaC) has been embraced by cloud providers and is a great opportunity to architect security into the design of a system (security by design) utilizing security best practices. However, too often, we see the on-premises mentality being applied to cloud deployments resulting in less secure systems instead of utilizing the security advantages a cloud provides. This course teaches the principles of Cloud Native security and how to avoid common pitfalls.

Course Outcomes

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Contents

1. Cloud security is different
   - 1.1 Shared responsibility model
   - 1.2 Infrastructure as code
   - 1.3 The Private, Public and Hybrid Cloud
   - 1.4 Types of virtualization
   - 1.5 Cloud threat models: Mitre Cloud ATT&CK

2. Losing the intranet
   - 2.1 Identify and Access Management
   - 2.2 Principle of least privilege and fine-grained cloud access control
   - 2.3 Using Software Defined Networks, virtual private clouds and subnets
   - 2.4 Moving to a serverless architecture
   - 2.5 Defense in depth

3. Security by design
   - 3.1 Orchestration: Infrastructure as Code
   - 3.2 The Automate-Everything principle, Updating and Repeatability
   - 3.3 Reuse of good design patterns
   - 3.4 Container security
   - 3.5 Identification and Authentication

4. Secure cloud coding
   - 4.1 Software supply chain security
   - 4.2 Continuous Integration and Deployment
   - 4.3 Testing in code integration for security
   - 4.4 Canaries in code deployment
   - 4.5 Policy engines

5. Confidentiality aspects
   - 5.1 Secrets management
   - 5.2 Encryption of data at rest
   - 5.3 Encryption of data in transit
   - 5.4 Data leakage and exfiltration

6. Availability
   - 6.1 Storage tiers and locality
   - 6.2 Backup strategies
   - 6.3 Data and process redundancy
   - 6.4 Data lifecycle configuration
   - 6.5 DDoS mitigation

7. Locality
   - 7.1 Compliance requirements
   - 7.2 Geography of data/processes
   - 7.3 Redundancy of data centers
   - 7.4 Colocation for performance reasons

8. Monitoring and Audit
   - 8.1 Centralized logging
   - 8.2 Auditing orchestration scripts
   - 8.3 Detecting misconfigurations
   - 8.4 Cloud Forensics

9. Summary and Research topics
   - 9.1 Homomorphic encryption
   - 9.2 Attestation
   - 9.3 Proof-carrying data
   - 9.4 Side-channel attacks
   - 9.5 Conclusions

Literature

Compulsory Reading

Further Reading

- Mitre Cloud ATT&CK. https://attack.mitre.org/matrices/enterprise/cloud/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Security by Design in the Cloud

Course Code: DLBCSEECS02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E

Course Description

This course provides the opportunity to implement a cloud software system using best cloud security practices. A list of ideas is provided on the online learning platform. In addition, the students can contribute use case ideas of their own after consulting with the tutor. The core aim is to apply the theoretical knowledge of cloud security methods and best practices to implement an application that is deployed as an Infrastructure-as-code project, can be monitored and audited, as well as easily and preferably automatically updated without danger. This entails reasoning about possible design and architectural choices in a rational way, as well as implementing them on a cloud platform, such as CNCF, Amazon AWS, Microsoft Azure or Google GCP.

Course Outcomes

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Contents

- This course is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Literature

Compulsory Reading

Further Reading

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Pentesting

Module Code: DLBCSEEPT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D ▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E	BA	10	300 h

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

Module Coordinator

N.N. (Principles of Ethical Hacking) / N.N. (Project: Pentesting)

Contributing Courses to Module

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

Module Exam Type

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

Weight of Module
see curriculum

Module Contents

Principles of Ethical Hacking

- History of ethical hacking
- Ethical and legal frameworks
- Planning phase
- Social Engineering & OSINT
- Tools
- RATs, Rootkits and Command & Control
- Data exfiltration
- Red/Blue Teams
- Bug Bounty programs
- Report writing

Project: Pentesting

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system.

Learning Outcomes

Principles of Ethical Hacking

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Project: Pentesting

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

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

Principles of Ethical Hacking

Course Code: DLBCSEEPT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Ethical hacking is an essential part in testing security implementations as well as discovering overlooked security issues. In this course, we will look at the principles and tools that hackers use and how ethical hacking is effectively utilized.

Course Outcomes

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Contents

1. History of ethical hacking

2. Ethical and legal frameworks
   - 2.1 Certifications
   - 2.2 Defining parameters of engagement
   - 2.3 Contracts

3. Planning phase
   - 3.1 Using Mitre PreATT&CK® for reconnaissance
   - 3.2 User Mitre Enterprise ATT&CK® for tool selection
   - 3.3 Documentation

4. Social Engineering & OSINT

5. Tools
   - 5.1 Web application pentesting tools
   - 5.2 Remote execution testing tools
   - 5.3 Password cracking
   - 5.4 OSINT tools
   - 5.5 Fuzzing tools
6. RATs, Rootkits and Command & Control
7. Data exfiltration
8. Red/Blue Teams
9. Bug Bounty programs
10. Report writing

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Pentesting

Course Code: DLBCSEEPT02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E

Course Description

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system. Students write a report outlining the vulnerabilities found, the methods used and proposals for fixing that class of vulnerability.

Course Outcomes

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Contents

- The student will be provided with virtual environments emulating corporate systems and an attacker machine with the necessary tools.

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBCSEEPT02_E

Industrielle Systemsicherheit

Modulcode: DLBCSEEIST_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	DLBINGEIT01 oder DLBINGEIT01_E	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

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

Kurse im Modul

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

Art der Prüfung(en)

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

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Grundlagen der industriellen Softwaretechnik

- Aufbau und Organisation von Informationssystemen
- Risiken und Herausforderungen der industriellen Softwaretechnik
- Softwarelebenszyklus: Von Planung bis Ablösung
- Requirements Engineering und Spezifikation
- Architektur und Implementierung
- Qualitätssicherung, Betrieb und Weiterentwicklung
- Rollen im Software Engineering
- Organisation von Softwareprojekten
- Softwareprozessmodell-Rahmenwerke

Sicherheit im Internet of Things

- Grundlagen des Internet der Dinge (IoT)
- Angriffe auf das Internet der Dinge
- Sicherheit durch Design
- Sichern von Geräten für das Internet der Dinge
- Operative Sicherheit
- Cloud-Sicherheit
- Große Daten / Künstliche Intelligenz

Qualifikationsziele des Moduls

Grundlagen der industriellen Softwaretechnik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einfache Berechnungen im Binärsystem (Boolsche Algebra) durchzuführen.
- den Aufbau von Rechnersystemen und Kommunikationsnetzen zu beschreiben.
- die Phasen eines SW-Lebenszyklus voneinander abzugrenzen.
- Rollen und Phasen im Software-Prozess voneinander abzugrenzen.
- verschiedene Vorgehensmodelle der SW-Entwicklung zu kennen.
- typische Herausforderungen und Risiken der industriellen SW-Entwicklung zu kennen.
- verschiedene Programmierparadigmen und deren Einsatz zu kennen.

Sicherheit im Internet of Things

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte von IoT-Architekturen zu kennen und zu verstehen.
- die gängigsten Schwachstellen, Bedrohungen und Risiken für das Internet der Dinge zu kennen und zu verstehen.
- Gegenmaßnahmen für IoT-Schwachstellen zu verstehen und anzuwenden.
- ein IoT-Architekturmodell/eine IoT-Lösung zu analysieren.

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

Grundlagen der industriellen Softwaretechnik

Kurscode: IGIS01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen Einblick in die technischen und theoretischen Grundlagen des Software Engineering zu vermitteln. Neben dem generellen Aufbau von Rechnersystemen werden den Studierenden typische Herausforderungen bei der Entwicklung industrieller Informationssysteme vermittelt. Darüber hinaus wird dargestellt, mit welchen typischen Phasen und Aktivitäten im Software Engineering diese Risiken gezielt adressiert werden.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- einfache Berechnungen im Binärsystem (Boolsche Algebra) durchzuführen.
- den Aufbau von Rechnersystemen und Kommunikationsnetzen zu beschreiben.
- die Phasen eines SW-Lebenszyklus voneinander abzugrenzen.
- Rollen und Phasen im Software-Prozess voneinander abzugrenzen.
- verschiedene Vorgehensmodelle der SW-Entwicklung zu kennen.
- typische Herausforderungen und Risiken der industriellen SW-Entwicklung zu kennen.
- verschiedene Programmierparadigmen und deren Einsatz zu kennen.

Kursinhalt

1. Aufbau und Organisation von Informationssystemen
   - 1.1 0 und 1 als Grundlage aller IT-Systeme
   - 1.2 Von-Neumann-Architektur
   - 1.3 Verteilte Systeme und Kommunikationsnetze
   - 1.4 Betriebliche Informationssysteme
2. Risiken und Herausforderungen der industriellen Softwaretechnik
   - 2.1 Eigenschaften von industriellen Softwaresystemen
   - 2.2 Softwaretechnik
   - 2.3 Risiken und typische Probleme
   - 2.4 Ursachenforschung
   - 2.5 Herausforderungen im Software Engineering

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Gumm, H. P./Sommer, M. (2011): Einführung in die Informatik. 9. Auflage, Oldenbourg, München. ▪ Hansen, H. R./Neumann, G. (2009): Wirtschaftsinformatik 1. Grundlagen und Anwendungen. 10. Auflage, UTB, Stuttgart. ▪ Ludewig, J./Lichter, H. (2010): Software Engineering. Grundlagen, Menschen, Prozesse, Techniken. 2. Auflage, dpunkt.verlag, Heidelberg. ▪ Sommerville, I. (2007): Software Engineering. 8. Auflage, Addison-Wesley, Boston.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Sicherheit im Internet of Things

Kurscode: DLBCSEEIST01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	DLBINGEIT01 oder DLBINGEIT01_E

Beschreibung des Kurses

Das Internet der Dinge (IoT) ist ein Megatrend. Er umfasst sowohl Endverbrauchersysteme als auch industrielle Systeme und Technologien (Industrial IoT, oder IIoT). Es gibt eine zunehmende Anzahl miteinander verbundener Geräte, aus denen sich das Internet der Dinge zusammensetzt. Im Allgemeinen besteht die Architektur des Internet der Dinge aus Endgeräten, Cloud-Lösungen und Akteuren/Sensoren. Die Sicherheit des Internet der Dinge bringt verschiedene Themen zusammen, d.h. Netzwerkprotokolle, Software, Hardware, Kryptographie und Cloud Computing.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Konzepte von IoT-Architekturen zu kennen und zu verstehen.
- die gängigsten Schwachstellen, Bedrohungen und Risiken für das Internet der Dinge zu kennen und zu verstehen.
- Gegenmaßnahmen für IoT-Schwachstellen zu verstehen und anzuwenden.
- ein IoT-Architekturmodell/eine IoT-Lösung zu analysieren.

Kursinhalt

1. Grundlagen des Internet der Dinge (IoT)
   - 1.1 Einführung
   - 1.2 Architektur
   - 1.3 Nicht-industrielles Internet der Dinge
   - 1.4 Industrie 4.0 (Industrielles IoT)
2. Angriffe auf das Internet der Dinge
   - 2.1 Verwundbarkeiten, Bedrohungen und Risiken
   - 2.2 Cyber-Angriffe und Gegenmaßnahmen
3. Sicherheit durch Design
   - 3.1 Projektmanagement / Sicherer Lebenszyklus der Entwicklung
   - 3.2 Statische Prüfung
   - 3.3 Dynamische Prüfung
   - 3.4 DevSecOps

4. Sichern von Geräten für das Internet der Dinge
   - 4.1 Sicherheitsrisiken
   - 4.2 Entwurfsziele
5. Operative Sicherheit
   - 5.1 Informations- und Cyber-Sicherheitsverwaltungssystem
   - 5.2 Netzwerk-Sicherheit
   - 5.3 Gerätekonfiguration
   - 5.4 Authentifizierung und Autorisierung
6. Cloud-Sicherheit
   - 6.1 Konzept des Nebels
   - 6.2 Bedrohungen für Cloud Internet of Things-Dienste
   - 6.3 Cloudbasierte Sicherheitsdienste
   - 6.4 Sichern der Cloud-Lösung
7. Big Data / Künstliche Intelligenz
   - 7.1 Beaufsichtigtes Lernen
   - 7.2 Unbeaufsichtigtes Lernen

Literatur

Pflichtliteratur

Weiterführende Literatur

- Butun, I. (2020): Industrial IoT. Challenges, Design Principles, Applications, and Security. 1st Edition, Springer International Publishing, Cham.
- Gupta B./Quamara, M. (2020): Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. 1st edition, CRC Press, Boca Raton, FL.
- Liyanage, M. et al. (2020): IoT Security. Advances in Authentication. 1st edition, John Wiley & Sons Ltd., Hoboken, NJ.
- Russell, B./Van Duren, D. (2018): Practical Internet of Things Security. Design a security framework for an Internet connected ecosystem. 2nd edition, Packt Publishing Ltd., Birmingham.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBCSEEIST01_D

Cyber Threat Intelligence

Module Code: DLBCSEECTI_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLBCSEECTI01_E	BA	10	300 h

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

Module Coordinator

N.N. (Attack Models and Threat Feeds) / N.N. (Project: Defense against APTs)

Contributing Courses to Module

- Attack Models and Threat Feeds (DLBCSEECTI01_E)
- Project: Defense against APTs (DLBCSEECTI02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Models and Threat Feeds • Study Format "Distance Learning": Exam, 90 Minutes Project: Defense against APTs • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Attack Models and Threat Feeds

- Apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model
- Determine what data is already available
- Do a gap analysis on what is detection or defense technology is missing
- Determine what extern threat feed data is required
- Utilize threat intelligence systems for diagnosis

Project: Defense against APTs

Using well-known methods like the MITRE ATT&CK Techniques, Tactics and Procedures students will be able to produce a comprehensive threat model. Therefore, students will have to determine through simulation or a “table top exercise” which data is already available and which extern threat feed data is required. After analyzing the “attack side” students will utilize threat intelligence systems for diagnostic to do a gap analysis – especially what defense technology is missing – and will be able to give sound advice to enhance resilience and to foster response capabilities. Emphasis will be drawn on the practical aspects of the defense against a given threat actor using techniques including beyond technical solutions and determine what cooperation with CERTs and ISPs is required to effectively defend against threats.

Learning Outcomes

Attack Models and Threat Feeds

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Project: Defense against APTs

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

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

Attack Models and Threat Feeds

Course Code: DLBCSEECTI01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, we look in depth at modeling threats and using data to diagnose, analyze and make recommendations. After a broad look at threat actors, we look at a variety of ways of modeling threats. This spans from Attack Trees to Kill Chains, but whichever method works the best, it all boils down to adversary Techniques, Tactics and Procedures. We look into the various taxonomies of these as defined by Mitre's ATT&CK and determine what can be observed in data.It is rare that internal data is enough for a complete analysis and in practice the threat analysist must use external data sources. These are available in a variety of formats, but the industry is converging on STIX and the use of software platforms like ACT to do the parsing and provide a good user experience.After looking at examples of threat actors and reports on them, we tackle the problem of making recommendations and writing reports. In some cases, engaging with law enforcement is required in which case some particularities need to be observed.

Course Outcomes

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Contents

1. Threat actors
   - 1.1 Script kiddies
   - 1.2 eCrime threat actors
   - 1.3 Advanced Persistent Threat actors (APT)
   - 1.4 Threat researchers

2. Modeling an attack
   - 2.1 Phases of an attack
   - 2.2 Lockheed Martin Kill-Chain
   - 2.3 Attack Trees
   - 2.4 STRIDE
   - 2.5 DREAD
   - 2.6 The Diamond Model of attack analysis
   - 2.7 Pyramid of pain
   - 2.8 Techniques, Tactics and Procedures

3. Attack preparation TTPs
   - 3.1 Observability of attack preparations
   - 3.2 Operational security of an organization

4. Enterprise TTPs
   - 4.1 Behaviors of the attacker
   - 4.2 Observable data in an enterprise

5. ICS TTPs
   - 5.1 Critical infrastructure
   - 5.2 Special considerations with IoT/ICS defense

6. Threat data exchange
   - 6.1 Indicators of Compromise
   - 6.2 Threat intelligence reports
   - 6.3 Ad-hoc data formats
   - 6.4 STIX format, TAXII protocol
   - 6.5 Mitre ATT&CK, CVEs, etc.
   - 6.6 The semantics of threat data
   - 6.7 Other sources of data for CTI analysis

7. Examples of threat analysis platforms
   - 7.1 ACT Platform
   - 7.2 MISP
   - 7.3 OpenCTI

8. Examples of threat actors and their modus operandi
   - 8.1 Threat model
   - 8.2 Relevant indicator data
   - 8.3 Relevant CTI data
   - 8.4 Diagnosing the threat
   - 8.5 Data coverage gap analysis

9. Reporting
   - 9.1 Mapping raw data to Mitre ATT&CK
   - 9.2 Making defensive recommendations
   - 9.3 Writing reports for technical staff
   - 9.4 Writing reports for management
   - 9.5 Working with law enforcement

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Defense against APTs

Course Code: DLBCSEECTI02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEECTI01_E

Course Description

This project course will give students hands-on experience in the challenging task to analyze threat vectors and real attacks of highly sophisticated, well planned, prepared and conducted attack campaigns named “Advanced Persistent Threats – APT´s” which derive from state, non-state or highly criminal attackers. Students will need to consider all practical aspects of different attack vectors using technical and non-technical (like social engineering) methods and procedures. To have the right understanding how to defend against these attacks they will use an attack simulator like Foreseeti SecureCAD or AttackIQ or conduct a “table top exercise” to figure out what data is required to analyze what security components and system configurations are needed to defend against a given, highly capable threat actor. Through this course, students will develop a complete overview what technical applications can be used to enhance resilience, foster response capabilities and recover from such attacks. Furthermore, students will have to take into account so called “soft measures” like organizational and procedural policies and regulations, bearing in mind the human factor in its social and psychological form. Through the cooperation with CERT´s, ISP´s and IT-Security Companies, academics and state agencies, students will cooperate on international level with IT-experts and experts from other disciplines to improve their expertise and to develop their personality.

Course Outcomes

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Contents

- This project course focuses on practical aspects how to defend against APTs. Students will start with a given use case to analyze a real-world APT Attack against a defined IT-System / Network, identify the different attack vectors on multiple levels and make the necessary data regarding used malware and exploits, techniques and procedures available by using a simulator or conducting a “table top exercise”. With this, students will develop a comprehensive picture of vulnerabilities and security shortfalls in the IT-system / network of

their own enterprise. Students will then have to analyze and identify what technical or non-technical measures could have prevented this attack using an interdisciplinary approach taking all levels and involved actors into account. Cooperation with other national and international CERT´s, ISP, IT-Security companies and state agencies will be the basis for a sound assessment how to improve the own resilience using best practices, state of the art technologies and considering new technologies.

- All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Telekommunikationspezifische Bedrohungen

Modulcode: DLBCSEEMT_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ keine ▪ DLBIBRVS01 oder DLBIBRVS01_E; DLBCSEINF01_D oder DLBCSEINF01_E	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. (Funk- und Telekommunikationssicherheit) / N.N. (Sofwarearchitektur mobiler Geräte)

Kurse im Modul

- Funk- und Telekommunikationssicherheit (DLBCSEEMT01_D)
- Sofwarearchitektur mobiler Geräte (DLBCSEEMT02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Funk- und Telekommunikationssicherheit • Studienformat "Fernstudium": Klausur, 90 Minuten Sofwarearchitektur mobiler Geräte • Studienformat "Fernstudium": Klausur, 90 Minuten

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Funk- und Telekommunikationssicherheit

- Überblick über drahtlose Protokolle
- Grundlagen von Drahtlosen Netwerken
- Telekommunikationsprotokoll-Klassen
- Telekom-Architektur
- Sicherheit von Handapparaten und Geräten
- Bedrohungen
- Andere drahtlose Anwendungen
- Schutzmaßnahmen

Sofwarearchitektur mobiler Geräte

- Mobil-Technologie-Stacks
- Hardware
- Android-Betriebssystem
- Apple iOS-Betriebssystem
- Mobile Geräte
- Software-Ökosysteme und Sicherheit
- Bedrohungen von Mobiltelefone
- Verwaltung mobiler Geräte

Qualifikationsziele des Moduls

Funk- und Telekommunikationssicherheit

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen der bei der Datenübertragung verwendeten drahtlosen Signale zu verstehen.
- verschiedene Arten der drahtlosen Vernetzung zu identifizieren und ihre Unterschiede zu verstehen.
- Telekommunikationsterminologie zu verstehen und diese der IT-Terminologie gegenüberzustellen.
- Architekturen der wichtigsten drahtlosen Telekommunikationssysteme zu verstehen.
- Angriffsvektoren gegen mobile Geräte sowie das Kernnetzwerk zu verstehen.
- andere Arten der Vernetzung, die möglicherweise genutzt werden, zu finden.

Sofwarearchitektur mobiler Geräte

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Hardware- und Software-Stacks gängiger Mobiltelefone zu verstehen.
- die Sicherheitskontrollen in diesen Stacks verstehen.
- zu erkennen, welche Schutzmaßnahmen und Risiken mit den Ökosystemen der Geräte verbunden sind.
- zu erkennen, welche Angriffe in der Vergangenheit erfolgreich waren.
- die Verwaltung mobiler Endgeräte zum Schutz eines Unternehmens zu nutzen.

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

Funk- und Telekommunikationssicherheit

Kurscode: DLBCSEEMT01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch	-1	5	DLBIBRVS01 oder DLBIBRVS01_E; DLBCSEINF01_D oder DLBCSEINF01_E

Beschreibung des Kurses

Die Zahl der Geräte, die drahtlos mit Netzwerken verbunden werden können, hat bereits die Zahl der Desktop- und Laptop-Computer überholt, die über ein Kabel mit einem lokalen Netzwerk verbunden sind. Vor allem Telefone und Tablets dominieren den Markt, die sich mit den drahtlosen Telekommunikationsnetzen verbinden. Es gibt aber auch viele andere Formen der drahtlosen Kommunikation, die von Geräten genutzt werden. Die Eigenheiten dieser drahtlosen Systeme müssen verstanden werden, um sie in ein vollständiges Sicherheitskonzept zu integrieren. Drahtlose Protokolle zwingen den User oft dazu, einem System zu vertrauen, in das er keinen Einblick hat. In diesem Kurs widmen wir uns genau diesem Thema.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen der bei der Datenübertragung verwendeten drahtlosen Signale zu verstehen.
- verschiedene Arten der drahtlosen Vernetzung zu identifizieren und ihre Unterschiede zu verstehen.
- Telekommunikationsterminologie zu verstehen und diese der IT-Terminologie gegenüberzustellen.
- Architekturen der wichtigsten drahtlosen Telekommunikationssysteme zu verstehen.
- Angriffsvektoren gegen mobile Geräte sowie das Kernnetzwerk zu verstehen.
- andere Arten der Vernetzung, die möglicherweise genutzt werden, zu finden.

Kursinhalt

1. Überblick über drahtlose Protokolle
   - 1.1 Netzwerkprotokolle für den persönlichen Bereich (Bluetooth, RFID, NFC und andere)
   - 1.2 Protokolle für drahtlose lokale Netzwerke (802.11a,b, g, ac , p und weitere)
   - 1.3 Wide Area Network-Protokolle (Telekommunikationsprotokolle, LoRa, Satellitenprotokolle und mehr)
   - 1.4 Schlüsselaustausch und Kryptographie in drahtlosen Netzwerken

2. Grundlagen von Drahtlosen Netwerken
   - 2.1 Frequenzen
   - 2.2 Modulationen
   - 2.3 Daten-Kodierungen
   - 2.4 Zielkonflikte

3. Telekommunikationsprotokoll-Klassen
   - 3.1 Telekommunikation vs. IT-Terminologie und -Technologien
   - 3.2 Telekommunikationsnormen
   - 3.3 Veraltete digitale Protokolle
   - 3.4 LTE
   - 3.5 5G

4. Telekom-Architektur
   - 4.1 Gesamtarchitektur
   - 4.2 Kern-Architektur
   - 4.3 Software-definierte Vernetzung
   - 4.4 5G-Campus-Netzwerke
   - 4.5 Sicherheit der Anwendungsschicht

5. Sicherheit von Handapparaten und Geräten
   - 5.1 Anforderungen
   - 5.2 Typischer Hardware-Entwurf
   - 5.3 IoT-Geräte

6. Bedrohungen
   - 6.1 Allgemeine Angriffsvektoren gegen (mobile) Geräte
   - 6.2 Allgemeine Angriffsvektoren gegen das Kernnetzwerk
   - 6.3 Mögliche Angriffe auf 5G-Campus-Netzwerke

7. Andere drahtlose Anwendungen
   - 7.1 Drahtlose Protokolle für Luftfahrt und Nautik
   - 7.2 Proprietäre Geräteprotokolle
   - 7.3 Großflächige Sensornetze (LoRa, Sigfox, ...)
   - 7.4 Digitale Sprach-/Datentechnologien (DECT/GAP, TETRA, ...)
   - 7.5 Satellitenkommunikation

8. Schutzmaßnahmen
   - 8.1 Mobile Technologie sicher integrieren
   - 8.2 Überwachung mobiler Geräte

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bartock, M. / Cichonski, J. / Souppaya, M. (2020): 5G CYBERSECURITY: Preparing a Secure Evolution to 5G.
- Cichonski, J. / Franklin, J. M. / Bartock, M. (2017): Guide to LTE Security. NIST Special Publication 800-187.
- Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/
- Pavur, J. et al. (2020): A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In 2020 IEEE Symposium on Security and Privacy (S&P). IEEE. May, 2020.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Sofwarearchitektur mobiler Geräte

Kurscode: DLBCSEEMT02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Mobile Geräte haben Desktops und Laptops als häufigste Endbenutzergeräte verdrängt. Das Smartphone ist zu einem zentralen Geschäftsinstrument geworden und User verwenden sie täglich für die unterschiedlichsten Anwendungen. Darüber hinaus nutzt auch das Internet der Dinge (IoT) diese mobilen Plattformen. Doch allzu oft sind die mit diesen mobilen Geräten verbundenen Risiken und Chancen insbesondere für die Sicherheitsadministratoren undurchsichtig, da diese Geräte oft außerhalb des traditionellen Intranets betrieben werden.In diesem Kurs untersuchen wir, wie die dominierenden Akteure, Android und Apple iOS, mit der Sicherheit in ihrem Softwarestack und ihrem Ökosystem umgehen. Wir betrachten auch das übersehene Problem der IoT-Sicherheit und schließen mit organisatorischen Lösungen ab.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Hardware- und Software-Stacks gängiger Mobiltelefone zu verstehen.
- die Sicherheitskontrollen in diesen Stacks verstehen.
- zu erkennen, welche Schutzmaßnahmen und Risiken mit den Ökosystemen der Geräte verbunden sind.
- zu erkennen, welche Angriffe in der Vergangenheit erfolgreich waren.
- die Verwaltung mobiler Endgeräte zum Schutz eines Unternehmens zu nutzen.

Kursinhalt

1. Mobil-Technologie-Stacks
   - 1.1 Hardware
   - 1.2 Firmware
   - 1.3 Betriebssystem
   - 1.4 Bewerbungen
   - 1.5 Ökosystem

2. Hardware
   - 2.1 RF-Module
   - 2.2 PDA-Modul
   - 2.3 Trusted Execution Environment
   - 2.4 Biometrische Geräte
   - 2.5 Standorttechnik

3. Android-Betriebssystem
   - 3.1 Hardware
   - 3.2 Bootloader
   - 3.3 Kernel- und Hardware-Abstraktionsschicht
   - 3.4 Sandboxing und Virtualisierung
   - 3.5 Code-Unterzeichnung

4. Apple iOS-Betriebssystem
   - 4.1 Hardware
   - 4.2 Bootloader
   - 4.3 Kernel und Frameworks
   - 4.4 Sandboxing und Virtualisierung
   - 4.5 Code-Unterzeichnung

5. Mobile Geräte
   - 5.1 Das Internet der Dinge
   - 5.2 Linux
   - 5.3 RTOS
   - 5.4 Android auf Geräten
   - 5.5 Andere gebräuchliche eingebettete Betriebssysteme

6. Software-Ökosysteme und Sicherheit
   - 6.1 Google Play
   - 6.2 Apple Store
   - 6.3 Sicherheitsanbieter
   - 6.4 Die Rolle der Cloud

7. Bedrohungen von Mobiltelefone
   - 7.1 Historische Beispiele für Angriffe auf Mobiltelefone
   - 7.2 Taxonomie der Bedrohungen von Mobiltelefonen
   - 7.3 Jailbreaking

8. Verwaltung mobiler Geräte
   - 8.1 Die Bedrohungen der BYOD
   - 8.2 Einzigartige Bedrohungen für mobile Geräte
   - 8.3 Verwaltung von Patches und Richtlinien

Literatur

Pflichtliteratur

Weiterführende Literatur

- Gupta, A. (2014): Learning Pentesting for Android Devices
- Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/
- N.A. (2020): Android Enterprise Security White Paper.
- N.A. (2019): iOS Security iOS 12.3. https://www.apple.com/lae/business/docs/site/iOS_Security_Guide.pdf
- Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Supply Chain Management

Modulcode: BWSC

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ keine	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Tobias Specker (Supply Chain Management I) / Prof. Dr. Tobais Specker (Supply Chain Management II)

Kurse im Modul

- Supply Chain Management I (BWSC01)
- Supply Chain Management II (BWSC02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Supply Chain Management I • Studienformat "Fernstudium": Klausur, 90 Minuten Supply Chain Management II • Studienformat "Fernstudium": Klausur, 90 Minuten

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Supply Chain Management I

- Historische und terminologische Aspekte zum SCM-Konzept
- Entstehungsmotive von unternehmensübergreifenden Wertschöpfungsnetzwerken
- Gestaltungsprinzipien und Effekte von Wertschöpfungsnetzwerken
- Logistische Kernprozesse und SCM
- Informationstechnische Aspekte des SCM-Konzeptes
- Koordination und Kollaboration der Netzwerkpartner
- Branchenspezifische Lösungen des SCM

Supply Chain Management II

- Strategische Aspekte des SCMs
- SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Planung
- SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Beschaffung
- SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Produktion
- SCM-Praxis: Aufgaben und Aktivitäten im Kernprozess Distribution

Qualifikationsziele des Moduls

Supply Chain Management I

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Bedeutung unternehmensübergreifender Wertschöpfungsprozesse zu erklären.
- gängige Konzepte zur Modellierung unternehmensübergreifender Wertschöpfungsprozesse zu erklären.
- die dynamischen Effekte in Supply Chains zu erläutern und deren Ursache bzw. Wirkungseffekte zu systematisieren.
- wichtige theoretische Konzepte zur Beschreibung der Merkmale und Herausforderungen unternehmensübergreifender Wertschöpfungsprozesse zu skizzieren.
- die im Kontext des Supply Chain Managements gängigen Zugänge und Problemkategorien zu erklären.
- wichtige Referenz- und/oder Managementmodelle zur Konkretisierung von Supply Chain Systemen zu benennen.
- wichtige Rollen und Aufgaben im SCM-Netzwerk zu erläutern.
- das Koordinationsproblem des SCM die diesbezüglich gängigen Lösungsansätze zu beschreiben.

Supply Chain Management II

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die strategische Relevanz unternehmensgreifender Wertschöpfungsprozesse in systematischer Weise zu erklären.
- die wichtigsten Aufgaben und Problem im SCM-Kernprozess Planung zu benennen.
- die Elemente und Zusammenhänge im CPFR-Modell in differenzierter Weise zu systematisieren.
- Merkmale und Besonderheiten der sog. Kontraktlogistik zu erläutern.
- die wichtigsten Aufgaben und Probleme im SCM-Kernprozess Beschaffung zu erklären.
- zentrale Elemente und Merkmale einer Beschaffungsstrategie zu erläutern.
- wichtigsten Aufgaben und Probleme im SCM-Kernprozess Produktion zu benennen.
- zentrale Elemente und Merkmale einer modernen Produktionsstrategie zu erläutern.
- die wichtigsten Aufgaben und Probleme im SCM-Kernprozess Distribution zu erklären.
- zentrale Elemente und Merkmale des sog. ECR-Konzeptes zu erläutern.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Baut auf Modulen aus dem Bereich Transport & Logistik auf	Alle Bachelor-Programme im Bereich Transport & Logistik

Supply Chain Management I

Kurscode: BWSC01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

SCM erweist sich aus theoretischer wie praktischer Sicht als ein überaus facettenreiches Konstrukt. Ein problemadäquates Verständnis der Problemdimensionen und Wirkungsweisen (globaler) unternehmensübergreifender Wertschöpfungsnetzwerke bedingt einen mehrdimensionalen Zugang. Dessen Ausgangspunkt bildet die Beschäftigung mit logistischen Prozessen. Das darin nach modernen Maßstäben angestrebte Denken in Prozessen, Strömen und Netzwerken bildet eine wichtige Basis des SCM. Auf der Grundlage eines solchen Zugangs sollen die Studierenden in grundsätzlicher Weise mit dem SCM-Konzept vertraut gemacht werden. Unter dem Gesichtspunkt einer ganzheitlichen Betrachtung erweist es sich ferner als sinnvoll, neben den logistischen Herausforderungen dieses Konzeptes eine Reihe weiterer typischer Problemfelder zu beleuchten. Dies betrifft zum einen die informationstechnischen Aspekte des SCM (bspw. also APS-Systeme), zum anderen Fragen der Kollaboration und Koordination der Netzwerkpartner. Vervollständigt wird dieser Abriss schließlich mit der Betrachtung ausgewählter branchenspezifischer SCM-Lösungen (bspw. also ECR oder VMI).

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Bedeutung unternehmensübergreifender Wertschöpfungsprozesse zu erklären.
- gängige Konzepte zur Modellierung unternehmensübergreifender Wertschöpfungsprozesse zu erklären.
- die dynamischen Effekte in Supply Chains zu erläutern und deren Ursache bzw. Wirkungseffekte zu systematisieren.
- wichtige theoretische Konzepte zur Beschreibung der Merkmale und Herausforderungen unternehmensübergreifender Wertschöpfungsprozesse zu skizzieren.
- die im Kontext des Supply Chain Managements gängigen Zugänge und Problemkategorien zu erklären.
- wichtige Referenz- und/oder Managementmodelle zur Konkretisierung von Supply Chain Systemen zu benennen.
- wichtige Rollen und Aufgaben im SCM-Netzwerk zu erläutern.
- das Koordinationsproblem des SCM die diesbezüglich gängigen Lösungsansätze zu beschreiben.

Kursinhalt

1. Grundsätzliches zum Supply Chain-Konzept
   - 1.1 Terminologische und konzeptionelle Grundlangen
   - 1.2 Supply Chain-Typologie nach Otto
   - 1.3 Supply Chain-Typologie nach Bechtel/Jayaram
   - 1.4 Dynamische Aspekte von Supply Chains

2. Ausgewählte theoretische Konzepte zum Supply Chain-Konzept
   - 2.1 Neue Institutionenökonomik
   - 2.2 Spieltheorie
   - 2.3 Netzwerksansatz
   - 2.4 Sonstige theoretische Zugänge

3. Supply Chain Management
   - 3.1 Grundsätzliches zu Zielen und Spannweite des SCM
   - 3.2 Populäre Problemfelder des SCM
   - 3.3 Supply Chain Management als Evolutionsstufe der Logistik
   - 3.4 Supply Chain Management als Kooperationsmanagement

4. SCM-Modell
   - 4.1 Grundsätzliches zum Begriff SCM-Modelle
   - 4.2 SCOR-Modell
   - 4.3 SCM-Aufgabenmodell

5. SCM als Koordinationsproblem
   - 5.1 Grundsätzliches zum Koordinationsbegriff
   - 5.2 Koordinationskonzepte, -kontext und -perspektiven des SCM
   - 5.3 Koordinationsinstrumente

Literatur

Pflichtliteratur

Weiterführende Literatur

- Arndt, H. (2018): Supply Chain Management. Optimierung logistischer Prozesse. 7. Auflage, Gabler, Wiesbaden.
- Beckmann, H. (2012): Prozessorientiertes Supply Chain Engineering. Strategien, Konzepte und Methoden zur modellbasierten Gestaltung. Gabler-Verlag | Springer Fachmedien, Wiesbaden.
- Heiserich, O.E./Helbig, K./Ullmann, W. (2011): Logistik. Eine praxisorientierte Einführung. 4. Auflage, Gabler-Verlag | Springer Fachmedien, Wiesbaden 2011.
- Hungenberg, H. (2014): Strategisches Management in Unternehmen. Ziele-Prozesse-Verfahren. 8. Auflage, Wiesbaden.
- Pfohl, H. C. (2010): Logistiksysteme. Betriebswirtschaftliche Grundlagen. 8 Auflage, Springer, Berlin.
- Schulte, C. (2013): Logistik. Wege zur Optimierung der Supply Chain. 6. Auflage, Vahlen, München.
- Werner, H. (2013): Supply Chain Management. Grundlagen, Strategien, Instrumente und Controlling. 5. Auflage, Gabler, Wiesbaden.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Supply Chain Management II

Kurscode: BWSC02

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	

Beschreibung des Kurses

Aus der Perspektive der strategischen Managementforschung und Praxis stehen die unter dem Begriff SCM gefassten Aktivitäten in enger Verbindung mit dem Bemühen zum Aufbau und/oder dem Erhalt erosionsstabiler betrieblicher Wettbewerbsvorteile. Eine grundsätzliche Erörterung dieses Zusammenhangs bildet den Ausgangspunkt dieses Kurses. Auf dieser Grundlage erfolgt danach im Rückgriff auf das sog. SCOR-Modell eine differenzierte Analyse von strategierelevanten Aktivitäten und Instrumenten im Bereich der Prozesskategorien Plan, Source, Make, Deliver und Return. Besondere Aufmerksamkeit wird dabei den praxisrelevanten Bereichen des SCMs gewidmet, bspw. also dem sog. Order-Promising (Plan), dem sog. Supplier-Relation-Management (Source), dem sog. Postponement (Make) oder dem sog. ECR-Konzept (Deliver).

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die strategische Relevanz unternehmensgreifender Wertschöpfungsprozesse in systematischer Weise zu erklären.
- die wichtigsten Aufgaben und Problem im SCM-Kernprozess Planung zu benennen.
- die Elemente und Zusammenhänge im CPFR-Modell in differenzierter Weise zu systematisieren.
- Merkmale und Besonderheiten der sog. Kontraktlogistik zu erläutern.
- die wichtigsten Aufgaben und Probleme im SCM-Kernprozess Beschaffung zu erklären.
- zentrale Elemente und Merkmale einer Beschaffungsstrategie zu erläutern.
- wichtigsten Aufgaben und Probleme im SCM-Kernprozess Produktion zu benennen.
- zentrale Elemente und Merkmale einer modernen Produktionsstrategie zu erläutern.
- die wichtigsten Aufgaben und Probleme im SCM-Kernprozess Distribution zu erklären.
- zentrale Elemente und Merkmale des sog. ECR-Konzeptes zu erläutern.

Kursinhalt

1. Strategische Aspekte des SCM
   - 1.1 Strategisches Denken und Handeln: Grundsätzliches
   - 1.2 Wettbewerbsschwerpunkt und SCM
   - 1.3 Wettbewerbsort und SCM
   - 1.4 Wettbewerbsregeln und SCM

2. SCM-Praxis: Kernprozess Planung
   - 2.1 Allgemeine Vorüberlegungen
   - 2.2 Collaborative Planning, Forecasting and Peplenishment
   - 2.3 Order Promising
   - 2.4 Kanban
   - 2.5 Integration von X-PL-Logistikdienstleistern

3. SCM-Praxis: Kernprozess Beschaffung
   - 3.1 Allgemeine Vorüberlegungen
   - 3.2 Produktionssynchrone Beschaffung
   - 3.3 Sourcing-Konzepte
   - 3.4 Supplier Relations Management

4. SCM-Praxis: Kernprozess Produktion
   - 4.1 Ausgewählte Aspekte zum Problemhintergrund
   - 4.2 Collaborative Engineering
   - 4.3 Postponement-Strategien
   - 4.4 Value Added Partnership

5. SCM-Praxis: Kernprozess Distribution
   - 5.1 Grundsätzliches zum Distributionsproblem
   - 5.2 Efficient Consumer Response (ECR)
   - 5.3 Konsignationslager

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Arndt, H. (2018): Supply Chain Management. Optimierung logistischer Prozesse. 7. Auflage, Gabler, Wiesbaden. ▪ Beckmann, H. (2012): Prozessorientiertes Supply Chain Engineering. Strategien, Konzepte und Methoden zur modellbasierten Gestaltung. Gabler-Verlag | Springer Fachmedien, Wiesbaden. ▪ Heiserich, O.E./Helbig, K./Ullmann, W. (2011): Logistik. Eine praxisorientierte Einführung. 4. Auflage, Gabler-Verlag | Springer Fachmedien, Wiesbaden 2011. ▪ Hungenberg, H. (2014): Strategisches Management in Unternehmen. Ziele-Prozesse-Verfahren. 8. Auflage, Wiesbaden. ▪ Pfohl, H. C. (2010): Logistiksysteme. Betriebswirtschaftliche Grundlagen. 8 Auflage, Springer, Berlin. ▪ Schulte, C. (2013): Logistik. Wege zur Optimierung der Supply Chain. 6. Auflage, Vahlen, München. ▪ Werner, H. (2013): Supply Chain Management. Grundlagen, Strategien, Instrumente und Controlling. 5. Auflage, Gabler, Wiesbaden.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Smart Factory

Modulcode: DLBINGSF

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Christian Magnus (Smart Factory I) / Prof. Dr. Christian Magnus (Smart Factory II)

Kurse im Modul

- Smart Factory I (DLBINGSF01)
- Smart Factory II (DLBINGSF02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Smart Factory I • Studienformat "Fernstudium": Klausur, 90 Minuten Smart Factory II • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Smart Factory I

- Motivation und Begriffsabgrenzung
- Entwicklung der Automatisierung
- Technologische Grundlagen und Standards
- Grundkonzepte einer Smart Factory
- Referenzarchitekturen
- Smart Factory Engineering
- Sicherheit

Smart Factory II

Die Studierenden bearbeiten eine selbstgewählte Aufgabenstellung mithilfe einer Prototyping-Umgebung, die zum Gegenstand der Aufgabenstellung passt. Sie dokumentieren ihr Ergebnis mit einem Projektbericht.

Qualifikationsziele des Moduls

Smart Factory I

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Begriff Smart Factory zu erläutern und in den Kontext Industrie 4.0 einzuordnen.
- die Entwicklung der Automatisierung bis zur vollautonomen, dezentral organisierten Produktionsanlage zu skizzieren.
- die grundlegenden Technologien und Standards zu benennen, die für den Entwurf und Betrieb einer Smart Factory eingesetzt werden.
- die wesentlichen Konzepte einer Smart Factory darzustellen.
- die einzelnen Elemente einer Smart Factory anhand verschiedener Referenzarchitekturen zu identifizieren und voneinander abzugrenzen.
- die besonderen Engineering-Herausforderungen im Smart Energy-Kontext herauszustellen.
- die speziellen sicherheitstechnischen Risiken digitalisierter und vernetzter Produktionsanlagen zu erläutern und ihnen jeweils konkrete Handlungsempfehlungen zuzuordnen.

Smart Factory II

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Technologien und Standards im Kontext Smart Factory zu durchdringen.
- Technologien im Kontext Smart Factory an einem einfachen Praxisbeispiel anzuwenden.
- zu einer ausgewählten Aufgabenstellung einen Hardware- oder Software-Prototypen zu entwerfen.
- Entwurfs- und Entwicklungstätigkeiten in Form eines Projektberichts zu dokumentieren.

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

Smart Factory I

Kurscode: DLBINGSF01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

In diesem Kurs sollen die Studierenden einen vertieften Einblick in die Vernetzung und Digitalisierung von Produktionsanlagen im Sinne einer Smart Factory erhalten. Hierzu werden sie mit den grundlegenden Zielen einer Smart Factory im Kontext des Forschungskomplexes Industrie 4.0 vertraut gemacht. Nach einer kurzen Einführung in die Geschichte der Automatisierung werden den Studierenden die technischen Grundlagen und Standards vermittelt, die für den Entwurf und den Betrieb einer Smart Factory erforderlich sind. Darauf aufbauend wird gezeigt, wie diese einzelnen Technologien eingesetzt werden, um die zentralen Konzepte einer Smart Factory zu realisieren. Um zu verstehen, aus welchen Bestandteilen eine Smart Factory besteht, werden verschiedene Referenzarchitekturen vor- und gegenübergestellt. Der Kurs schließt mit den besonderen Engineering-Herausforderungen einer autonom handelnden und dezentral organisierten Produktionsanlage. Dazu zählt vor allem der Aspekt der IT-Sicherheit, der durch die digitale Vernetzung der Produktionsanlagen und Produkte besonders relevant ist.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Begriff Smart Factory zu erläutern und in den Kontext Industrie 4.0 einzuordnen.
- die Entwicklung der Automatisierung bis zur vollautonomen, dezentral organisierten Produktionsanlage zu skizzieren.
- die grundlegenden Technologien und Standards zu benennen, die für den Entwurf und Betrieb einer Smart Factory eingesetzt werden.
- die wesentlichen Konzepte einer Smart Factory darzustellen.
- die einzelnen Elemente einer Smart Factory anhand verschiedener Referenzarchitekturen zu identifizieren und voneinander abzugrenzen.
- die besonderen Engineering-Herausforderungen im Smart Energy-Kontext herauszustellen.
- die speziellen sicherheitstechnischen Risiken digitalisierter und vernetzter Produktionsanlagen zu erläutern und ihnen jeweils konkrete Handlungsempfehlungen zuzuordnen.

Kursinhalt

1. Motivation und Begriffsabgrenzung
   - 1.1 Ziele von Smart Factory
   - 1.2 Internet of Things
   - 1.3 Cyber-physische Systeme
   - 1.4 Cyber-physische Produktionssysteme
   - 1.5 Smart Factory als Cyber-physisches (Produktions-)System

2. Entwicklung der Automatisierung
   - 2.1 Automatisierungspyramide
   - 2.2 Vernetzte, dezentrale Organisation der Produktion
   - 2.3 Zukünftige Herausforderungen

3. Technologische Grundlagen und Standards
   - 3.1 Identifizierung physikalischer Objekte
   - 3.2 Formale Beschreibungssprachen und Ontologien
   - 3.3 Digitales Objektgedächtnis
   - 3.4 Physikalische Situationserkennung
   - 3.5 (Teil-)autonomes Handeln und Kooperieren
   - 3.6 Mensch-Maschine-Interaktion
   - 3.7 Maschine-Maschine-Kommunikation

4. Grundkonzepte einer Smart Factory
   - 4.1 Auftragsgesteuerte Produktion
   - 4.2 Bündelung von Maschinen- und Produktionsdaten
   - 4.3 Unterstützung des Menschen in der Produktion
   - 4.4 Intelligente Produkte und Betriebsmittel
   - 4.5 Smart Services

5. Referenzarchitekturen
   - 5.1 Zweck und Eigenschaften von Referenzarchitekturen
   - 5.2 Überblick über Normungsinitiativen
   - 5.3 CyProS-Referenzarchitektur
   - 5.4 RAMI 4.0 (DIN SPEC 91345)

6. Smart Factory Engineering
   - 6.1 Klassifikation verschiedener Engineering-Werkzeuge
   - 6.2 Virtual Engineering
   - 6.3 User-Centered Design
   - 6.4 Requirements Engineering
   - 6.5 Modellierung
   - 6.6 Integration klassischer und smarter Komponenten

7. Sicherheit
   - 7.1 Sicherheitsrisiken in einer Smart Factory
   - 7.2 Handlungsvorschläge des BMWi
   - 7.3 VDMA-Handlungsleitfaden

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bangemann, T. et al. (2016): Integration of Classical Components into Industrial Cyber–Physical Systems. In: Proceedings of the IEEE, 104. Jg., Heft 5, S. 947–959. DOI: 10.1109/JPROC.2015.2510981.
- Bauernhansl, T./Hompel, M. ten/Vogel-Heuser, B. (Hrsg.) (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Springer, Berlin.
- Bundesministerium für Wirtschaft und Energie (Hrsg.) (2016): IT-Sicherheit für die Industrie 4.0. Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten. Berlin.
- Geisberger, E./Broy, M. (Hrsg.) (2012): agendaCPS. Integrierte Forschungsagenda Cyber-Physical Systems. Springer, Berlin/Heidelberg.
- Harrison, R./Vera, D./Ahmad, B. (2016): Engineering Methods and Tools for Cyber–Physical Automation Systems. In: Proceedings of the IEEE, 104. Jg., Heft 5, S. 973–985. DOI: 10.1109/JPROC.2015.2510665.
- Haupert, J. (2013): DOMeMan: Repräsentation, Verwaltung und Nutzung von digitalen Objektgedächtnissen. Akademische Verlagsgesellschaft AKA, Berlin.
- VDMA & Partner (2016): Leitfaden Industrie 4.0 Security. Handlungsempfehlungen für den Mittelstand. VDMA Verlag, Frankfurt a. M.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☑ Vodcast	☐ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Smart Factory II

Kurscode: DLBINGSF02

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

In diesem Kurs wählen die Studierenden in Abstimmung mit dem Seminarleiter eine konkrete Aufgabenstellung aus dem bereitgestellten Themenkatalog aus. Sie bearbeiten die Aufgabe mithilfe einer Prototyping-Umgebung, die zum Gegenstand der Aufgabenstellung passt. Bei den Umgebungen kann es sich sowohl um Hardware (z. B. Prototyping-Boards) als auch um Software (z. B. technologiespezifische Entwicklungsumgebungen) handeln. Zur Bearbeitung der Aufgabe wenden die Studierenden die im Kurs Smart Factory I vermittelten Konzepte, Methoden und Werkzeuge an. Sie dokumentieren ihr Ergebnis mit einem Projektbericht.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Technologien und Standards im Kontext Smart Factory zu durchdringen.
- Technologien im Kontext Smart Factory an einem einfachen Praxisbeispiel anzuwenden.
- zu einer ausgewählten Aufgabenstellung einen Hardware- oder Software-Prototypen zu entwerfen.
- Entwurfs- und Entwicklungstätigkeiten in Form eines Projektberichts zu dokumentieren.

Kursinhalt

- Ein Katalog mit den jeweils aktuell bereitgestellten Aufgabenstellungen wird auf der Online-Plattform des Moduls bereitgestellt. Er bietet die inhaltliche Basis des Moduls und kann vom Seminarleiter ergänzt bzw. aktualisiert werden.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Themenspezifische Literaturauswahl

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☑ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLBINGSF02

Robotics und Automatisierung

Modulcode: DLBCSDWRA

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Mario Boßlau (Fertigungsverfahren Industrie 4.0) / Prof. Dr. Matthias Eifler (Automatisierung und Robotics)

Kurse im Modul

- Fertigungsverfahren Industrie 4.0 (DLBINGFVI01)
- Automatisierung und Robotics (DLBINGAUR01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Fertigungsverfahren Industrie 4.0 • Studienformat "Fernstudium": Klausur, 90 Minuten • Studienformat "Kombistudium": Klausur, 90 Minuten Automatisierung und Robotics • Studienformat "Kombistudium": Klausur, 90 Minuten • Studienformat "Fernstudium": Klausur, 90 Minuten

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Fertigungsverfahren Industrie 4.0

- Einführung in die Fertigungstechnik
- Fertigungshauptgruppen nach DIN 8580
- Additive Fertigungsverfahren
- Rapid Prototyping
- Rapid Tooling
- Direct/Rapid Manufacturing
- Cyber-physische Produktionsanlagen

Automatisierung und Robotics

- Grundlagen der Automatisierung
- Grundlagen der Messtechnik
- Sensoren
- Grundlagen der Regelungstechnik
- Grundlagen der Steuerungstechnik
- Einführung in die Robotik
- Kinematik eines Roboters

Qualifikationsziele des Moduls

Fertigungsverfahren Industrie 4.0

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Begriffe und Zusammenhänge der Fertigungstechnik zu erklären.
- die aktuellen Veränderungen in der Fertigungstechnik durch Technologien wie der Additiven Fertigung und Megatrends wie Cyber Physical Systems darzustellen.
- verschiedene Fertigungsverfahren den Fertigungshauptgruppen nach DIN 8580 zuzuordnen.
- das grundlegende Prinzip additiver Fertigungsverfahren zu erklären.
- verschiedene additive Fertigungsverfahren voneinander abzugrenzen.
- die Begriffe Rapid Prototyping, Rapid Tooling und Direct Manufacturing zu erläutern und ihnen jeweils einzelne Verfahren und Anwendungsbeispiele zuzuordnen.
- die Elemente und Eigenschaften Cyber-physischer Produktionsanlagen zu erklären.

Automatisierung und Robotics

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Aspekte der Automatisierung zu erläutern.
- die verschiedenen Größen und Einheiten in der Messtechnik zu benennen.
- verschiedene Messmethoden voneinander abzugrenzen.
- den grundlegenden Aufbau von Messeinrichtungen zu beschreiben.
- einen geeigneten Sensor anhand verschiedener Kriterien auszuwählen.
- die Elemente von Regelungssystemen zu benennen.
- das Verhalten von Regelsystemen im Zeit- und Frequenzbereich zu beschreiben.
- grundlegende Prinzipien der Steuerungstechnik zu beschreiben.
- zwischen verschiedenen Zahlensystemen umzurechnen und die Boolesche Algebra anzuwenden.
- den Aufbau von Schaltnetzen, -werken und Speichern zu beschreiben.
- wichtige Elemente von Steuerungssystemen wie Signalgeneratoren und Leistungsverstärker zu benennen.
- einfache speicherprogrammierbare Steuerungen zu entwerfen.
- den grundlegenden Aufbau von Industrierobotern zu beschreiben.
- verschiedene Bewegungen und Positionen von Gelenkarmrobotern zu berechnen.

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

Fertigungsverfahren Industrie 4.0

Kurscode: DLBINGFVI01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden, ausgehend von traditionellen, standardisierten Fertigungstechniken, einen Überblick über solche Verfahren zu bieten, die durch technologische Entwicklungen unter dem Oberbegriff Industrie 4.0 die Produktionsprozesse beeinflusst haben und noch beeinflussen. Dazu zählen insbesondere technologische Fortschritte bei den additiven Fertigungsverfahren, die Anwendungen wie das Rapid Prototyping, Rapid Tooling und das Direct Manufacturing ermöglichen. Abschließend behandelt der Kurs die Folgen der Digitalisierung und Vernetzung von Produktionsanlagen und deren Elemente im Sinne eines Cyber-physischen Systems.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Begriffe und Zusammenhänge der Fertigungstechnik zu erklären.
- die aktuellen Veränderungen in der Fertigungstechnik durch Technologien wie der Additiven Fertigung und Megatrends wie Cyber Physical Systems darzustellen.
- verschiedene Fertigungsverfahren den Fertigungshauptgruppen nach DIN 8580 zuzuordnen.
- das grundlegende Prinzip additiver Fertigungsverfahren zu erklären.
- verschiedene additive Fertigungsverfahren voneinander abzugrenzen.
- die Begriffe Rapid Prototyping, Rapid Tooling und Direct Manufacturing zu erläutern und ihnen jeweils einzelne Verfahren und Anwendungsbeispiele zuzuordnen.
- die Elemente und Eigenschaften Cyber-physischer Produktionsanlagen zu erklären.

Kursinhalt

1. Einführung in die Fertigungstechnik
   - 1.1 Grundlegende Begriffe und Zusammenhänge in der Fertigungslehre
   - 1.2 Historische Entwicklung der Fertigung
   - 1.3 Die Diskussion über den Long Tail

2. Fertigungshauptgruppen nach DIN 8580
   - 2.1 Urformen
   - 2.2 Umformen
   - 2.3 Trennen (Zerteilen, Zerspanung, Abtragen)
   - 2.4 Fügen
   - 2.5 Beschichten
   - 2.6 Stoffeigenschaftsändern

3. Additive Fertigungsverfahren
   - 3.1 Grundprinzip und rechtliche Aspekte
   - 3.2 Stereolithographie (STL)
   - 3.3 Selektives Lasersintern und selektives Strahlschmelzen mit Laser- oder Elektronenstrahl
   - 3.4 Fused Deposition Modeling (FDM)
   - 3.5 Multi-Jet Modeling (MJM) und Poly-Jet-Verfahren (PJM)
   - 3.6 3D-Druckverfahren (3DP)
   - 3.7 Laminierverfahren
   - 3.8 Maskensintern

4. Rapid Prototyping
   - 4.1 Begriffsbestimmung
   - 4.2 Strategische und operative Aspekte
   - 4.3 Anwendungsgebiete und -beispiele

5. Rapid Tooling
   - 5.1 Begriffsbestimmung, strategische und operative Aspekte
   - 5.2 Indirekte und direkte Verfahren

6. Direct/Rapid Manufacturing
   - 6.1 Potentiale und Anforderungen an die Verfahren
   - 6.2 Umsetzung, Anwendungsgebiete und -beispiele

7. Cyber-physische Produktionsanlagen
   - 7.1 Herleitung der Begriffe Industrie 4.0 und Cyber-physische Systeme
   - 7.2 Megatrend Cyber Physical Systems (CPS)
   - 7.3 Definition Cyber-physische Produktionsanlage
   - 7.4 Auswirkungen auf Planung und Betrieb von Produktionsanlagen
   - 7.5 Dynamische Rekonfiguration und Migration von Produktionsanlagen

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Anderson, C. (2012): Makers. The new industrial revolution. Crown Business, New York. ▪ Bauernhansl, Thomas/Hompel, M. ten/Vogel-Heuser, B. (Hrsg.) (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung – Technologien – Migration. Springer, Wiesbaden. ▪ Gebhardt, A. (2012): Understanding Additive Manufacturing. Rapid Prototyping – Rapid Tooling – Rapid Manufacturing. Hanser, München/Cincinnati. ▪ Lachmayer, R./Lippert, R. B./Fahlbusch, T. (Hrsg.) (2016): 3D-Druck beleuchtet. Additive Manufacturing auf dem Weg in die Anwendung. Springer, Berlin/Heidelberg. ▪ Wittenstein, M. et al. (Hrsg.) (2015): Intelligente Vernetzung in der Fabrik. Industrie 4.0. Umsetzungsbeispiele für die Praxis. Fraunhofer Verlag, Stuttgart.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Automatisierung und Robotics

Kurscode: DLBINGAUR01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Ziel des Kurses ist es, den Studierenden einen Einblick in die Mess-, Regel- und Steuerungstechnik zu bieten sowie die Grundlagen der Robotik zu vermitteln. Hierzu wird den Studierenden dargelegt, mit welchen Methoden bestimmte Messgrößen ermittelt werden können und wie mit Messfehlern umgegangen wird. Auf diesen Grundlagen aufbauend werden verschiedene Sensoren vorgestellt und die Studierenden dazu befähigt, passende Sensoren anhand vorgegebener Kriterien auszuwählen. Der Kurs führt die Studierenden darüber hinaus in die Grundlagen der Regelungstechnik ein. Dabei werden den Studierenden die verschiedenen Möglichkeiten zur Beschreibung der Struktur und des Verhaltens von Regelsystemen veranschaulicht. Neben der Regelungstechnik werden auch die Grundlagen der Steuerungstechnik vermittelt. Die Studierenden erhalten eine kurze Einführung in binäre Zahlensysteme und die Boolesche Algebra und setzen sich darüber hinaus mit verschiedenen basalen Schaltungs- und Steuerungselementen auseinander. Zuletzt erhalten die Studierenden einen Einblick in die Robotik mit einem Schwerpunkt auf Industrieroboter. In diesem Zusammenhang erlernen die Studierenden die Beschreibung und Berechnung von Positionen und Bewegungen einzelner Glieder eines Roboterarms.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegenden Aspekte der Automatisierung zu erläutern.
- die verschiedenen Größen und Einheiten in der Messtechnik zu benennen.
- verschiedene Messmethoden voneinander abzugrenzen.
- den grundlegenden Aufbau von Messeinrichtungen zu beschreiben.
- einen geeigneten Sensor anhand verschiedener Kriterien auszuwählen.
- die Elemente von Regelungssystemen zu benennen.
- das Verhalten von Regelsystemen im Zeit- und Frequenzbereich zu beschreiben.
- grundlegende Prinzipien der Steuerungstechnik zu beschreiben.
- zwischen verschiedenen Zahlensystemen umzurechnen und die Boolesche Algebra anzuwenden.
- den Aufbau von Schaltnetzen, -werken und Speichern zu beschreiben.
- wichtige Elemente von Steuerungssystemen wie Signalgeneratoren und Leistungsverstärker zu benennen.
- einfache speicherprogrammierbare Steuerungen zu entwerfen.
- den grundlegenden Aufbau von Industrierobotern zu beschreiben.
- verschiedene Bewegungen und Positionen von Gelenkarmrobotern zu berechnen.

Kursinhalt

1. Grundlagen der Automatisierung
   - 1.1 Grundlegende Begriffe
   - 1.2 Wirtschaftliche Aspekte
   - 1.3 Automatisierungspyramide
   - 1.4 Mess-, Steuer- und Regelsysteme

2. Grundlagen der Messtechnik
   - 2.1 Messgrößen und Einheiten
   - 2.2 Formen von Messsignalen
   - 2.3 Messmethoden
   - 2.4 Messeinrichtungen
   - 2.5 Bewertung von Messungen und Messfehler

3. Sensoren
   - 3.1 Funktion und Elemente von Sensoren
   - 3.2 Kriterien zur Auswahl von Sensoren
   - 3.3 Näherungsschalter
   - 3.4 Fotoelektrische Sensoren
   - 3.5 Ultraschallsensoren
   - 3.6 Drehgeber
   - 3.7 Kraft-, Drehmoment- und Druckmesser
   - 3.8 Temparatursensoren
   - 3.9 Bildverarbeitende Sensoren

4. Grundlagen der Regelungstechnik
   - 4.1 Elemente von Regelungssystemen
   - 4.2 Strukturbeschreibung
   - 4.3 Statische Verhaltensbeschreibung
   - 4.4 Verhaltensbeschreibung im Zeitbereich
   - 4.5 Verhaltensbeschreibung im Frequenzbereich
   - 4.6 Praxisbeispiele

5. Grundlagen der Steuerungstechnik
   - 5.1 Grundprinzip und Elemente von Steuerungssystemen
   - 5.2 Zahlendarstellungen
   - 5.3 Boolesche Algebra
   - 5.4 Schaltnetze, -werke und Speicher
   - 5.5 Signalgeneratoren und Leistungsverstärker
   - 5.6 Speicherprogrammierbare Steuerungen
   - 5.7 Verbindungsprogrammierte Steuerungen

6. Einführung in die Robotik
   - 6.1 Begriffe und Einordnung
   - 6.2 Grundlegende Elemente
   - 6.3 Klassifikation von Robotern

7. Kinematik eines Roboters
   - 7.1 Koordinatensysteme und Bezugspunkte
   - 7.2 Rotationen
   - 7.3 Vorwärts- und Rückwärtstransformationen

Literatur

Pflichtliteratur

Weiterführende Literatur

- Heinrich, B./Linke, P./Glöckler, M. (2015): Grundlagen Automatisierung. Springer, Wiesbaden.
- Hesse, S./Malisa, V. (Hrsg.) (2016): Taschenbuch Robotik – Montage – Handhabung. 2. Auflage, Carl Hanser Verlag, München.
- Jazar, R. N. (2010): Theory of Applied Robotics. 2. Auflage, Springer US, Boston (MA).
- Karaali, C. (2013): Grundlagen der Steuerungstechnik. Springer, Wiesbaden.
- Parthier, R. (2011): Messtechnik. Grundlagen und Anwendungen der elektrischen Messtechnik für alle technischen Fachrichtungen und Wirtschaftsingenieure. 6. Auflage, Vieweg & Teubner, Wiesbaden.
- Tietze, U./Schenk, C./Gamm, E. (2016): Halbleiter-Schaltungstechnik. 15. Auflage, Springer, Berlin.
- Zacher, S./Reuter, M. (2014): Regelungstechnik für Ingenieure. Springer, Wiesbaden.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden

- ☐ Learning Sprints®
- ☑ Skript
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☑ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☐ Prüfungsleitfaden
- ☑ Live Tutorium/Course Feed

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLBINGAUR01

Mobile Software Engineering

Modulcode: IWMB

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

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Marian Benner-Wickner (Mobile Software Engineering am Beispiel der Android-Plattform) / Prof. Dr. Marian Benner-Wickner (Projekt Mobile Software Engineering)

Kurse im Modul

- Mobile Software Engineering am Beispiel der Android-Plattform (IWMB01)
- Projekt Mobile Software Engineering (IWMB02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Mobile Software Engineering am Beispiel der Android-Plattform • Studienformat "Fernstudium": Klausur, 90 Minuten Projekt Mobile Software Engineering • Studienformat "Kombistudium": Schriftliche Ausarbeitung: Projektbericht • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Mobile Software Engineering am Beispiel der Android-Plattform

- Grundlagen der mobilen Software-Entwicklung
- Android-Systemarchitektur
- Entwicklungsumgebung
- Kernkomponenten einer Android-App
- Interaktion zwischen Anwendungskomponenten
- Fortgeschrittene Techniken

Projekt Mobile Software Engineering

Konzeption, Umsetzung und Dokumentation von kleinen, mobilen Anwendungen auf Basis einer konkreten Aufgabenstellung.

Qualifikationsziele des Moduls

Mobile Software Engineering am Beispiel der Android-Plattform

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Unterschiede und Besonderheiten der SW-Entwicklung für mobile Systeme zu erkennen und diese zu erläutern.
- verschiedene Aktivitäten, Rollen und Risiken bei Erstellung, Betrieb und Wartung von mobilen Software-Systemen zu unterscheiden.
- Architektur und technische Eigenschaften der Android Plattform zu erläutern und zu unterscheiden.
- selbstständig mobile Software-Systeme zur Lösung von konkreten Problemen für die Plattform „Android“ zu erstellen.

Projekt Mobile Software Engineering

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstststständig eine kleine mobile Anwendung zu konzipieren und prototypisch zu erstellen, um eine gezielte Aufgabe zu lösen.
- typische Probleme und Herausforderungen in der praktischen Umsetzung kleiner mobiler Anwendungen zu erkennen.
- die Konzeption und die Umsetzung von kleinen, eigenständig konzipiert und umgesetzten mobilen Anwendungen zu dokumentieren.

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

Mobile Software Engineering am Beispiel der Android-Plattform

Kurscode: IWMB01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Am Beispiel der mobilen Plattform „Android“ wird vermittelt, wie sich die Programmierung von mobilen Anwendungen (Apps) von der Entwicklung von Browser-basierten Informationssystemen unterscheidet, welche Technologien und Programmierkonzepte typischerweise dabei zum Einsatz kommen und welche typischen Herausforderungen es bei der App-Entwicklung für industrielle Anwendungen gibt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Unterschiede und Besonderheiten der SW-Entwicklung für mobile Systeme zu erkennen und diese zu erläutern.
- verschiedene Aktivitäten, Rollen und Risiken bei Erstellung, Betrieb und Wartung von mobilen Software-Systemen zu unterscheiden.
- Architektur und technische Eigenschaften der Android Plattform zu erläutern und zu unterscheiden.
- selbstständig mobile Software-Systeme zur Lösung von konkreten Problemen für die Plattform „Android“ zu erstellen.

Kursinhalt

1. Grundlagen der mobilen Software-Entwicklung
   - 1.1 Besonderheiten von mobilen Endgeräten
   - 1.2 Besonderheiten der mobilen Software-Entwicklung
   - 1.3 Einteilung von mobilen Endgeräten
   - 1.4 Die Android-Plattform
2. Android-Systemarchitektur
   - 2.1 Das Android-System
   - 2.2 Sicherheit
   - 2.3 Kommunikation mit Netzwerken

3. Entwicklungsumgebung
   - 3.1 Android Studio
   - 3.2 Erste App und Emulator-Test
   - 3.3 Anwendungsdeployment

4. Kernkomponenten einer Android-App
   - 4.1 Überblick über die Komponenten einer Android-App
   - 4.2 Activities, Layouts und Views
   - 4.3 Ressourcen
   - 4.4 Zusammenfassung in einer App
   - 4.5 Grafische Gestaltung

5. Interaktion zwischen Anwendungskomponenten
   - 5.1 Intents
   - 5.2 Services
   - 5.3 Broadcast Receive

6. Fortgeschrittene Techniken
   - 6.1 Threading
   - 6.2 Anwendungsspeicher

Literatur

Pflichtliteratur

Weiterführende Literatur

- Becker, A./Pant, M. (2015): Android 5. Programmieren für Smartphones und Tablets. 4. Auflage, dpunkt.verlag, Heidelberg.
- Eason, J. (2014): Android Studio 1.0. (URL: https://android-developers.googleblog.com/2014/12/android-studio-10.html [letzter Zugriff: 12.06.2015]).
- Franke, F./Ippen, J. (2012): Apps mit HTML5 und CSS3. Galileo Computing, Bonn.
- Google Inc. (Hrsg.) (2015): Android Developer Guide. (URL: http://developer.android.com/guide [letzter Zugriff: 12.06.2015]).
- Google Inc. (Hrsg.) (2015): App Components. (URL: http://developer.android.com/guide/components/index.html [letzter Zugriff: 12.06.2015]).
- Google Inc. (Hrsg.) (2015): Installing the Android SDK. (URL: http://developer.android.com/sdk/installing/index.html [letzter Zugriff: 13.05.2015]).
- Google Inc. (Hrsg.) (2015): Resources Overview. (URL: http://developer.android.com/guide/topics/resources/overview.html [letzter Zugriff: 12.06.2015]).
- Hipp, Wyrick & Company, Inc. (Hrsg.) (2015): SQLite Webseite. (URL: http://sqlite.org/index.html [letzter Zugriff: 12.06.2015]).
- Künneth, T. (2015): Android 5. Apps entwickeln mit Android Studio. 3. Auflage, Rheinwerk Computing, Bonn.
- Post, U. (2014): Android Apps entwickeln. 4. Auflage, Galileo Computing, Bonn.
- Ross, M. (2013): Phone Gap. Mobile Cross-Plattform-Entwicklung mit Apace Cordova & Co. dpunkt.verlag, Heidelberg.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt Mobile Software Engineering

Kurscode: IWMB02

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		5	keine

Beschreibung des Kurses

Die Studierenden erstellen selbständig eine mobile Anwendung und dokumentieren deren Konzeption und Umsetzung.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- selbstständig eine kleine mobile Anwendung zu konzipieren und prototypisch zu erstellen, um eine gezielte Aufgabe zu lösen.
- typische Probleme und Herausforderungen in der praktischen Umsetzung kleiner mobiler Anwendungen zu erkennen.
- die Konzeption und die Umsetzung von kleinen, eigenständig konzipiert und umgesetzten mobilen Anwendungen zu dokumentieren.

Kursinhalt

- Konzeption, Umsetzung und Dokumentation von kleinen, mobilen Anwendungen auf Basis einer konkreten Aufgabenstellung.
  Mögliche Themen sind zum Beispiel:
- Eine Radio-App, um den Austausch zwischen Hörer und Sender allgemein, aber vor allem zwischen Hörern und Radiomoderatoren zu verbessern.
- Eine App, mit der eine Gruppe von Brettspielfans ihren regelmäßigen abendlichen Spieltermin besser organisieren kann.
- Eine App, mit der die Betreuer von Abschlussarbeiten an der IUBH ihre Betreuungsprozesse verbessern können.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Becker, A./Pant, M. (2015): Android 5. Programmieren für Smartphones und Tablets. 4. Auflage, dpunkt, Heidelberg.
- Eason, J. (2014): Android Studio 1.0. (URL: http://android-developers.blogspot.de/2014/12/android- studio-10.html [letzter Zugriff: 12.06.2015]).
- Franke, F./Ippen, J. (2012): Apps mit HTML5 und CSS3. Rheinwerk Verlag, Bonn.
- Google Inc. (Hrsg.) (2015): Android Developer Guide. (URL: http://developer.android.com/guide)
- Google Inc. (Hrsg.) (2015a): App Components. (URL: http://developer.android.com/guide/components/ index.html [letzter Zugriff: 12.06.2015]).
- Google Inc. (Hrsg.) (2015b): Installing the Android SDK. (URL: http://developer.android.com/sdk/ installing/index.html [letzter Zugriff: 13.05.2015]).
- Google Inc. (Hrsg.) (2015c): Resources Overview. (URL: http://developer.android.com/guide/topics/ resources/overview.html [letzter Zugriff: 12.06.2015]).
- Hipp, Wyrick & Company, Inc. (Hrsg.) (2015): SQLite Webseite. (URL: http://sqlite.org/index.html [letzter Zugriff: 12.06.2015]).
- Künneth, T. (2016): Android 7. Das Praxisbuch für Entwickler. 4. Auflage, Rheinwerk, Bonn.
- Ross, M. (2013): Apache Cordova. Eine praktische Einführung in die mobile Cross-Plattform-Entwicklung mit PhoneGap. dpunkt Verlag, Heidelberg.
- Post, U. (2014): Android Apps entwickeln. Eigene Spiele-Apps für Leser mit Programmierkenntnissen. 4. Auflage, Galileo Computing, Bonn.

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden

- ☐ Learning Sprints®
- ☐ Skript
- ☐ Vodcast
- ☐ Shortcast
- ☐ Audio
- ☐ Musterklausur
- ☐ Repetitorium
- ☐ Creative Lab
- ☑ Prüfungsleitfaden
- ☐ Live Tutorium/Course Feed

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

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

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

Bachelorarbeit

Modulcode: BBAK

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	gemäß Studien- und Prüfungsordnung	BA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Studiengangleiter (SGL) (Bachelorarbeit) / Studiengangsleiter (SGL) (Kolloquium)

Kurse im Modul

- Bachelorarbeit (BBAK01)
- Kolloquium (BBAK02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Bachelorarbeit • Studienformat "Fernstudium": Bachelorarbeit • Studienformat "Kombistudium": Bachelorarbeit Kolloquium • Studienformat "Fernstudium": Kolloquium • Studienformat "Kombistudium": Kolloquium

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Bachelorarbeit

- Bachelorarbeit
- Kolloquium zur Bachelorarbeit

Kolloquium

Qualifikationsziele des Moduls

Bachelorarbeit

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kolloquium

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Beachtung akademischer Präsentations- und Kommunikationstechniken vorzustellen.
- das in der Bachelorarbeit gewählte wissenschaftliche und methodisch Vorgehen reflektiert darzustellen.
- themenbezogene Fragen der Fachexperten (Gutachter der Bachelorarbeit) aktiv zu beantworten.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Alle Module	Alle Bachelor-Programme im Fernstudium

Bachelorarbeit

Kurscode: BBAK01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		9	gemäß Studien- und Prüfungsordnung

Beschreibung des Kurses

Ziel und Zweck der Bachelorarbeit ist es, die im Verlauf des Studiums erworbenen fachlichen und methodischen Kompetenzen in Form einer akademischen Abschlussarbeit mit thematischem Bezug zum Studienschwerpunkt erfolgreich anzuwenden. Inhalt der Bachelorarbeit kann eine praktisch-empirische oder aber theoretisch-wissenschaftliche Problemstellung sein. Studierende sollen unter Beweis stellen, dass sie eigenständig unter fachlich-methodischer Anleitung eines akademischen Betreuers eine ausgewählte Problemstellung mit wissenschaftlichen Methoden analysieren, kritisch bewerten und Lösungsvorschläge erarbeiten können. Das von dem Studierenden zu wählende Thema aus dem jeweiligen Studienschwerpunkt soll nicht nur die erworbenen wissenschaftlichen Kompetenzen unter Beweis stellen, sondern auch das akademische Wissen des Studierenden vertiefen und abrunden, um seine Berufsfähigkeiten und -fertigkeiten optimal auf die Bedürfnissen des zukünftigen Tätigkeitsfeldes auszurichten.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

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

Kursinhalt

- Die Bachelorarbeit muss zu einer Themenstellung geschrieben werden, die einen inhaltlichen Bezug zum jeweiligen Studienschwerpunkt aufweist. Im Rahmen der Bachelorarbeit müssen die Problemstellung sowie das wissenschaftliche Untersuchungsziel klar herausgestellt werden. Die Arbeit muss über eine angemessene Literaturanalyse den aktuellen Wissensstand des zu untersuchenden Themas widerspiegeln. Der Studierende muss seine Fähigkeit unter Beweis stellen, das erarbeitete Wissen in Form einer eigenständigen und problemlösungsorientierten Anwendung theoretisch und/oder empirisch zu verwerten.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Hunziker, A.W. (2010): Spaß am wissenschaftlichen Arbeiten. So schreiben Sie eine gute Semester-, Bachelor- oder Masterarbeit. 4. Auflage, Verlag SKV, Zürich. ▪ Wehrlin, U. (2010): Wissenschaftliches Arbeiten und Schreiben. Leitfaden zur Erstellung von Bachelorarbeit, Masterarbeit und Dissertation – von der Recherche bis zur Buchveröffentlichung. AVM, München. ▪ Themenabhängige Literaturauswahl

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Thesis-Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Bachelorarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
270 h	0 h	0 h	0 h	0 h	270 h

Lehrmethoden
Selbstständige Projektbearbeitung unter akademischer Anleitung.

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Thesis-Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Bachelorarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
270 h	0 h	0 h	0 h	0 h	270 h

Lehrmethoden
Selbstständige Projektbearbeitung unter akademischer Anleitung.

Kolloquium

Kurscode: BBAK02

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
BA	Deutsch		1	Gemäß Studien- und Prüfungsordnung

Beschreibung des Kurses

Das Kolloquium wird nach Einreichung der Bachelorarbeit durchgeführt. Es erfolgt auf Einladung der Gutachter. Im Rahmen des Kolloquiums müssen die Studierenden unter Beweis stellen, dass sie den Inhalt und die Ergebnisse der schriftlichen Arbeit in vollem Umfang eigenständig erbracht haben. Inhalt des Kolloquiums ist eine Präsentation der wichtigsten Arbeitsinhalte und Untersuchungsergebnisse durch den Studierenden sowie die Beantwortung von Fragen der Gutachter.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Beachtung akademischer Präsentations- und Kommunikationstechniken vorzustellen.
- das in der Bachelorarbeit gewählte wissenschaftliche und methodisch Vorgehen reflektiert darzustellen.
- themenbezogene Fragen der Fachexperten (Gutachter der Bachelorarbeit) aktiv zu beantworten.

Kursinhalt

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

Literatur

Pflichtliteratur

Weiterführende Literatur

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

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Kolloquium

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Kolloquium

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
30 h	0 h	0 h	0 h	0 h	30 h

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung

Studienformat Kombistudium

Studienform	Kursart
Kombistudium	Kolloquium

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Kolloquium

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
30 h	0 h	0 h	0 h	0 h	30 h

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung