HOCHSCHULE ANSBACH

Modulbeschreibungen B.Sc. Datenschutz und IT-Sicherheit (DIS)

Inhalt

Teil I (Fachsemester 1 und 2)

Pflichtmodule (PM)

PM: Einführung in die IT-Sicherheit

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Einführung in die IT-Sicherheit
Modulverantwortliche(r):	Prof. Dr. Jens Söldner
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	240 Stunden, davon: 72 Stunden Präsenzzeit, 168 Stunden Vor- und Nachbereitung und Selbststudium und Prüfungsvorbereitung
ECTS-Punkte:	8
Semesterwochenstunden:	6
Veranstaltungstyp:	6 SWS Vorlesung und seminaristischer Unterricht
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 Min.)

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden verfügen über ein breites Grundlagenwissen im Bereich IT-Sicherheit, welches sie u.a. zur Teilnahme an weiterführenden Lehrveranstaltungen befähigt. Die Studierenden besitzen ein grundlegendes Verständnis wichtiger Einsatzgebiete der IT-Sicherheit in einer Organisation und kennen die typischen Problemstellungen und Lösungsansätze der Informatik dafür. Darauf aufbauend verfügen die Studierenden über die Fähigkeit Entwicklungen und Tendenzen im Bereich der IT-Sicherheit kritisch zu hinterfragen und Querbeziehungen zu erkennen.

Handlungskompetenz
Die Studierenden können grundlegende fachliche Entscheidungen in den behandelten Bereichen selbständig treffen. Sie besitzen zudem die Fähigkeit sich eigenständig in Fachgebiete zielgerichtet einzuarbeiten und die dazu notwendigen Informationen zu beschaffen. Die Studierenden können bei der Auswahl von IT-Sicherheitswerkzeugen bzw. -Appliances, Methoden oder Konzepten aktiv mitwirken, um den operativen Betrieb einer Organisation möglichst sicher zu gestalten. Basierend auf der erworbenen Fachkompetenz können die Studierenden im 4. Fachsemester eine fundierte Wahl der Studienschwerpunkte treffen.

Sozialkompetenz
Aufbauend auf Ihren Erfahrungen in der Lehrveranstaltung besitzen die Studierenden die Fähigkeit Fachprobleme in Kleingruppen zu diskutieren und eigene Lösungsvorschläge im Kollegenkreis zielgerichtet zu vermitteln.

Inhalt:

- Motivation IT-Sicherheit: Aktuelle Fälle der IT-Sicherheit – Vorstellung, Recherche
- Bedrohungsszenarien, grundlegende Angriffsvektoren, z.B.
  - Social Engineering
  - Hacking
  - (Distributed) Denial of Service (DDOS)
- Erster Einstieg in die Kryptoanalyse:
  - Brute-Force
  - Wörterbuchangriff, Rainbow tables
  - Man-in-the-Middle

- Grundbegriffe der IT-Sicherheit: Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit, Zurechnbarkeit/Accountability, Access Control, etc.
- Standards in der IT-Sicherheit: IT-Sicherheitsmanagement, Grundschutzkatalog BSI, ISO 27001
- Biometrie, Authentifizierung, Zugriffs-/Zugangangskontrolle
- Der Faktor Mensch in der IT-Sicherheit, Awareness IT-Sicherheit
- Notfallplanung, Response, Veröffentlichung
- Ausblick / Motivation Datenschutz

Literatur:

- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle, 10th expanded and updated edition (21. August 2018), De Gruyter Verlag, ISBN: 978-3110551587
- Michael Kofler et al.: Hacking & Security: Das umfassende Handbuch, 1. Auflage (27. April 2018), Verlag Rheinwerk Computing, ISBN: 978-3836245487
- Tom DeMarco, Timothy R. Lister: „Wien wartet auf Dich! -Der Faktor Mensch im DV-Management“ (engl. „Peopleware“), 2. Auflage, Hanser Verlag, ISBN: 3-446-21277-9

PM: Datenschutzrecht I

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Datenschutzrecht I
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Schulkenntnisse
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Vorlesung und seminaristischer Unterricht
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

Qualifikationsziele:

Fach- und Methodenkompetenz

Die Studierenden verfügen über Grundlagenwissen im Bereich des Datenschutzrechts, welches sie u.a. zur Teilnahme an weiterführenden Lehrveranstaltungen befähigt. Die Studierenden besitzen ein grundlegendes Verständnis wichtiger Prinzipien und Konstituenten des Datenschutz- und IT-Rechts, kennen die typischen Fragestellungen im Kontext der EU-DSGVO und nachfolgender Rechtsvorschriften. Darauf aufbauend verfügen die Studierenden über die Fähigkeit Entwicklungen und Tendenzen im Bereich des Datenschutzrechts kritisch hinterfragen und Querbeziehungen erkennen zu können.

Handlungskompetenz

Die Studierenden können weitgehend eigenständig einfach Fragestellungen im Bereich des Datenschutzrechts beantworten, bzw. Antworten begründet herleiten. Sie sind weiterhin in der Lage typische Fragestellungen in Organisationen als relevant für eine Datenschutzrechtliche Betrachtung zu erkennen.

Sozialkompetenz

Die Studierenden können die Prinzipien des modernen Datenschutzes allgemeinverständlich erklären und plausibel herleiten. Aufbauend darauf können Sie in einer Organisation für grundlegendes Verständnis und Awareness bzgl. der täglichen Umsetzung des Datenschutzes sorgen.

Inhalt:

- Rechtliche Grundlagen

- Grundsätze des Datenschutzrechts
- Rechte der Betroffenen
- Verantwortliche und Auftragsverarbeiter
- BDSG-neu & Erwägungsgründe
- IT- und Computerrecht
- Typische/Beispielhafte Fragestellungen in der Praxis

Literatur:

- Ivo Geis, et al.: Datenschutzrecht, 11. Auflage (15. Oktober 2018), dtv Verlagsgesellschaft, ISBN: 978-3423057721
- Jürgen Kühling et al.: Datenschutzrecht (Start ins Rechtsgebiet), 4., völlig neu bearbeitete Auflage 2018 (28. März 2018), ISBN: 978-3811445710
- Bayerisches Landesamt für Datenschutzaufsicht (Herausgeber), Thomas Kranig, Eugen Ehmann: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket, 1. Auflage (17. November 2017), Verlag C.H.Beck, ISBN: 978-3406716621
- Helmut Redeker: IT-Recht, 6. Auflage, neubearbeitete (28. November 2016), C.H.Beck Verlag, ISBN: 978-3406687273
- DSK-Kurzpapiere (https://www.datenschutzkonferenz-online.de/kurzpapiere.html)

PM: Datenschutzrecht II

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Datenschutzrecht II
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Modul Datenschutzrecht I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Sommersemester
Unterrichtsprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

Qualifikationsziele:

Fach- und Methodenkompetenz

Die Studierenden verfügen über vertieftes Wissen im Bereich des Datenschutzrechts und angrenzender Rechtsfelder. Die Studierenden besitzen ein umfassendes Verständnis der wichtigsten Rechtsvorschriften und können Rechtsfragen den einzelnen Rechtsgebieten zuordnen. Die Studierenden sind selbstständig in der Lage weitergehende Recherchen im Kontext des Datenschutzrechts durchzuführen und können klar Gültigkeiten und Zuständigkeiten abgrenzen.

Handlungskompetenz

Die Studierenden können weitgehend eigenständig fortgeschrittene Fragestellungen im Bereich des Datenschutzrechts und angrenzender Rechtsgebiete beantworten, bzw. Antworten begründet herleiten. Sie sind weiterhin in der Lage für typische Fragestellungen in Organisationen zu erkennen wann weitergehendes juristisches Fachwissen notwendig ist, bzw. wann ggf. Aufsichtsbehörden einzuschalten sind.

Sozialkompetenz

Die Studierenden können auch im vertieften Fachgespräch unter KollegInnen folgen und aktiv daran

teilnehmen. Aufbauend darauf können Sie in einer Organisation an rechtskonformen Regelungen für den Datenschutz mitarbeiten.
Inhalt: • Verhaltensregeln und Zertifizierung • Vertiefung Datenschutzrecht und angrenzende Rechtsgebiete wie z.B. Telemediengesetz, Telekommunikationsgesetz • Übermittlung in Drittländer • Aufgaben der Aufsichtsbehörden • Sanktionen
Literatur: ● Ivo Geis, et al.: Datenschutzrecht, 11. Auflage (15. Oktober 2018), dtv Verlagsgesellschaft, ISBN: 978-3423057721 ● Geppert et al.: Telemediarecht Telekommunikations- und Multimediarecht: Telekommunikationsgesetz. Rahmenrichtlinie. Telekommunikations-Überwachungsverordnung. Netzwerkdurchsuchungsgesetz, 11. Auflage (8. Dezember 2017), dtv Beck Texte, ISBN: 978-3423055987 ● DSK-Kurzpapiere (https://www.datenschutzkonferenz-online.de/kurzpapiere.html)

PM: Kryptographie

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Kryptographie
Modulverantwortliche(r):	Prof. Dr.-Ing. Sascha Müller-Feuerstein
Vorkenntnisse:	Modul Mathematik
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht und Übung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

Qualifikationsziele:

Fach- und Methodenkompetenz

Die Studierenden kennen die Bedeutung der wichtigsten kryptographischen Verfahren und kennen ihre typischen Einsatzbereiche. Die Studierenden verstehen die grundlegenden Konzepte der wichtigsten Verschlüsselungs-, Hash- und Authentifizierungsverfahren und die typischen Angriffsvektoren / Schwächen dieser Verfahren.

Handlungskompetenz

Die Studierenden können die grundlegenden Prinzipien kryptographischer Verfahren auch in neuen Verfahren erkennen und diese grob klassifizieren. Die Studierenden verstehen die prinzipiellen Vorteile, aber auch die Risiken des unsachgemäßen Einsatzes von kryptographischen Verfahren. Die Studierenden sind in der Lage zu erkennen, wann vertiefte fachliche Expertise zu Rate gezogen werden sollte.

Sozialkompetenz

Die Studierenden können einfachen Fachgesprächen zu den behandelten Konzepten folgen und in Diskussionen mit anderen Studierenden aktiv teilnehmen. Die Studierenden können die grundlegenden Prinzipien der symmetrischen und asymmetrischen Verschlüsselung, sowie des Hashings allgemeinverständlich erklären.

Inhalt:

- Entwicklung der Kryptographie, bekannte Fälle (Enigma), Motivation
- Abgrenzung Steganographie
- Mathematische Grundlagen
- Symmetrische & asymmetrische Kryptographie
  - AES, DES, IDEA, PGP, RSA, Diffie-Hellmann, ElGamal, Elliptic Curve
  - Attacken, Brute Force, Rainbow Tables, Man-in-the-Middle
- Hashingverfahren
  - MD5, SHA-Familie, etc.
  - Secure Password Management
- Authentifizierungsverfahren, z.B. Challenge-Response, Zero-Knowledge-Verfahren
- Anwendung, z.B. in der Blockchain (Merkletree, Nonce)
- Praktikum/Übung: Angewandte Kryptographie
  - Einsatz und Übungen mit u.a. Cryptool (https://www.cryptool.org/de/), Hashgenerator (https://hashgenerator.de/)

Literatur:

- Bruce Schneier: Angewandte Kryptographie, 1. Auflage (1. Dezember 2005), Pearson Studium Verlag, ISBN: 978-3827372284
- Stephan Spitz et al.: Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen, 2. Auflage, überarb. Aufl. 2011 (24. Februar 2011), Vieweg+Teubner Verlag, ISBN: 978-3834814876
- Ronald Petrlic et al.: Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie,1. Auflage (10. April 2017), Springer Vieweg Verlag, ISBN: 978-3658168384

PM: Programmierung I

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Programmierung I
Modulverantwortliche(r):	Prof. Dr. Schön
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	210 Stunden, davon: 72 Stunden Präsenzzeit, 138 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	7
Semesterwochenstunden:	6
Veranstaltungstyp:	2 SWS Vorlesung mit 4 SWS Übung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 min)

Qualifikationsziele:

Fach- und Methodenkompetenz

Die Studierenden können einfache Programme in einer höheren Programmiersprache entwickeln und wenden dabei die Prinzipien der strukturierten Programmierung an. Sie verstehen es, geeignete Sprachelemente bei der Umsetzung von Programmierproblemen in lauffähige Programme zu verwenden.

Handlungskompetenz

Die Studierenden können einfache Programme (Konsolprogramme) für betriebliche Aufgabenstellungen entwerfen und implementieren.

Inhalt:

- Programmiersprachen allgemein (Arten, Konzepte)
- Grundlegende Einführung in die Syntax und Semantik einer höheren Programmiersprache (elementare und komplexe Datentypen, Anweisungen, Kontrollstrukturen), Einsatz von Programmbibliotheken;

- Einführung in die Grundlagen der objektorientierten Programmierung (Klassen, Objekte, Attribute, Methoden);
- Entwicklungsmethodik für das Programmieren im Kleinen, schrittweise Verfeinerung, Prinzipien der strukturierten Programmierung;
- Einführung in eine moderne Entwicklungsumgebung für das Erstellen, Verwalten und Testen von Programmen;

Literatur:

- H. Mössenböck: Sprechen Sie Java? dpunkt.verlag, jeweils neuste Auflage
- Ratz, Scheffler, Seese, Wiesenberger: Grundkurs Programmieren in Java, Hanser, jeweils neuste Auflage
- Fritz Jobst: Programmieren in Java, Hanser, jeweils neuste Auflage
- Guido Krüger: Java-Programmierung – das Handbuch, O'Reilly, jeweils neuste Auflage
- Christian Ullenboom: Java ist auch eine Insel, Galileo Computing, jeweils neuste Auflage
- T. Künneth: Einstieg in ECLIPSE: Werkzeuge für Java-Entwickler, Galileo Computing, 2014

PM: Programmierung II

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Programmierung II
Modulverantwortliche(r):	Prof. Dr. Schön
Vorkenntnisse:	Programmierung I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	6
Veranstaltungstyp:	2 SWS Vorlesung mit 2 SWS Übung
Semesterturnus:	Sommersemester
Unterrichtsprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 min)

Qualifikationsziele:

Fach- und Methodenkompetenz

Vertiefung der Fähigkeiten, die in Programmieren I erworben wurden. Die Studierenden beherrschen die Grundlagen und Konzepte der objektorientierten Programmierung und können diese in mindestens einer objektorientierten Programmiersprache anwenden.

Handlungskompetenz

Die Studierenden können Programme (Konsolprogramme, grafisch-interaktive) für anspruchsvolle betriebliche Aufgabenstellungen entwerfen und implementieren.

Inhalt:

- Einführung in die „Paradigmen" der objektorientierten Programmierung (assoziative Beziehungen, Vererbung, Aggregation, Schnittstellen)
- Vertiefung in objektorientierte Programmiertechniken (Polymorphismus, Kommunikation zwischen den Objekten, einfache Design-Pattern, Model-View-Controller Konzept (MCV), typische Datenstrukturen, Benutzung von Klassenbibliotheken, grafische Benutzeroberflächen).
- Einführung in die funktionale Programmierung

Literatur:

- H. Mössenböck: Sprechen Sie Java? dpunkt.verlag, jeweils neuste Auflage
- Ratz, Scheffler, Seese, Wiesenberger: Grundkurs Programmieren in Java, Hanser, jeweils neuste Auflage
- Fritz Jobst: Programmieren in Java, Hanser, jeweils neuste Auflage

- Guido Krüger: Java-Programmierung – das Handbuch, O'Reilly, jeweils neuste Auflage
- Christian Ullenboom: Java ist auch eine Insel, Galileo Computing, jeweils neuste Auflage
- T. Künneth: Einstieg in ECLIPSE: Werkzeuge für Java-Entwickler, Galileo Computing, 2014
- Anton Epple: JavaFX 8, Grundlagen und fortgeschrittene Techniken, dpunkt.verlag, 2016

PM: Grundlagen der Informatik

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Grundlagen der Informatik
Modulverantwortliche(r):	Prof. Dr. Knüpffer, Prof. Dr.-Ing. Sascha Müller-Feuerstein
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 min)

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden haben einen umfassenden Überblick über die wichtigsten Aspekte moderner Betriebs- und Kommunikationssysteme. Sie kennen die Anforderungen an moderne Betriebssysteme und die Grundkonzepte für deren Lösung in verschiedenen Betriebssystemen. Sie haben das Prinzip der Abstraktion durch Definition von Netzwerkschichten verinnerlicht und können aktuelle Kommunikationstechnologien vor dem Hintergrund ihrer historischen Entwicklung einordnen und verstehen.

Handlungskompetenz
Die Studierenden können im Rahmen des Aufbaus von IT-Lösungen in einfachen Kommunikationsszenarien Empfehlungen für die Auswahl geeigneter Betriebssysteme und Kommunikationsmittel aussprechen. Aufgrund des erworbenen Grundwissens sind sie in der Lage, auch zukünftige Entwicklungen in diesen Bereichen einzuordnen und zu bewerten.

Inhalt:
Das Modul ist in zwei Teile gegliedert. Unter anderem werden folgende Themen behandelt:

<u>Teil I: Betriebssysteme:</u>
- Einführung in die Architektur moderner Betriebssysteme,
- Methoden der Prozess- und Betriebsmittelsteuerung,
- Methoden zur Hauptspeicherverwaltung,
- Aufbau moderner Dateiverwaltungssysteme und Methoden der Dateiverwaltung.

<u>Teil II: Kommunikationssysteme:</u>
- Darstellung wesentlicher Entwicklungen im Bereich der Kommunikationstechnik,
- Funktionen von Kommunikationssystemen, Netzwerktopologien und – technologien,
- Netzwerk-Protokolle, Netzwerk-Referenzmodellen (ISO/OSI, TCP/IP),
- Algorithmen und Strategien für das Routing, Netzlaststeuerung,
- Fehlerbehandlung, Zugriffssteuerung,
- Anwendungsprotokolle (HTTP, IMAP, POP3, FTP, etc.),
- Netzwerkgeräte (Hub, Bridge, Switch, Router, Gateway, etc.).

Literatur:

Übergreifende Literatur:

- Hansen, R., Neumann G.: Wirtschaftsinformatik 2; Informationstechnik. 9. Auflage.Lucius & Lucius. Stuttgart 2005.

Zu Teil I:

- Brause, R.: Betriebssysteme - Grundlagen und Konzepte. Springer-Verlag, Berlin-Heidelberg, 2. Auflage, 2013. ISBN 3540009000
- Stallings, W.: Betriebssysteme – Prinzipien und Umsetzung. Prentice Hall. 4. Auflage, 2003. ISBN 3-8273-7030-2
- A.-S. Tanenbaum: Moderne Betriebssysteme. Addison-Wesley Longman, 4. Auflage, 2016. ISBN 3-8273-70719-1

Zu Teil II:

- Andrew, S. Tanenbaum, David J. Wetherall: Computernetzwerke. Pearson
- James, F. Kurose, Keith W. Ross: Computernetzwerke: Der Top-Down-Ansatz. Pearson
- Schreiner, R.: Computernetzwerke, Von den Grundlagen zur Funktion und Anwendung. Hanser

PM: Cyber Security

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Cyber Security
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Modul Grundlagen der IT-Sicherheit
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht und Übung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz:

Handlungskompetenz:

Sozialkompetenz:

Inhalt:

- Analyse mit Wireshark, Überwachung mit Nagios
- Einsatz von speziellen Sicherheits-OSen, wie z.B. Kali-Linux
- Penetration-Testing, z.B. Metasploit
- TLS/SSL, SSL-Zertifikate
- Tracking-Tools
- Datenschutz und Sicherheitsanforderungen an Webseiten, z.B. OWASP Top 10

Literatur:

- Michael Bartsch et al.: Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden, 1. Auflage 2018 (8. August 2018), Springer Vieweg Verlag, ISBN: 978-3658216542
- Mark B.: Hacken mit Kali-Linux: Schnelleinstieg für Anfänger, 1. Auflage (1. November 2017), Books on

Demand Verlag, ISBN: 978-3746012650
- Laura Chappel: Wireshark® 101: Einführung in die Protokollanalyse - Deutsche Ausgabe, 2. Auflage 2018 (31. Januar 2018), mitp Verlag, ISBN: 978-3958456839
- K. Benedikt, A. Buckel, J. Mammen: DS-GVO und ePrivacy-VO auf Webseiten umsetzen

PM: Mathematik

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Mathematik
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Schulwissen (allgemeine oder fachgebundene Hochschulreife)
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Vorlesung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 min)

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden beherrschen die mathematischen Grundlagen, die als Instrumentarium in den verschiedenen fachspezifischen Modulen benötigt werden.

Handlungskompetenz
Die Studierenden sind in der Lage, das Instrumentarium der Mathematik anzuwenden, um Problemstellungen im Umfeld der Ökonomie zu analysieren und zu lösen.

Inhalt:

Lineare Algebra
Lineare Gleichungssysteme; Matrizen und Vektoren; Grundlagen der Linearen Optimierung.

Analysis
Differentialrechnung mit einer und mit mehreren unabhängigen Veränderlichen, d.h.: Diskussion der bei ökonomischen Anwendungen wichtigsten Funktionen, Extremwertbestimmung ohne und mit Nebenbedingungen; Integralrechnung samt deren ökonomischen Anwendungen.

Mathematische Grundlagen der Kryptographie
Polynom-Resteklassen, Potenzen modulo n, Sätze von Fermat und Euler, diskreter Logarithmus.

Literatur

- Schwarze, Jochen: Mathematik für Wirtschaftswissenschaftler, 5 Bände, Verlag Neue Wirtschaftsbriefe (NWB)
- Holland, Heinrich und Doris Holland: Mathematik im Betrieb, Gabler-Verlag
- Tietze, Jürgen: Einführung in die angewandte Wirtschaftsmathematik, Vieweg-Verlag
- Ohse, Dieter: Mathematik für Wirtschaftswissenschaftler, 2 Bände, Verlag Franz Vahlen
- 5. Rommelfanger, Heinrich: Mathematik für Wirtschaftswissenschaftler, 2 Bände, Spektrum Akademischer Verlag

PM: Algorithmen & Datenstrukturen

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Algorithmen & Datenstrukturen
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Programmierung I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Vorlesung und seminaristischer Unterricht
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

Qualifikationsziele:

Fach- und Methodenkompetenz

Grundlegende Datenstrukturen und die dazugehörigen Algorithmen kennen und verstehen. Einfache Algorithmen analysieren, beschreiben und auf Korrektheit prüfen können. Algorithmen hinsichtlich ihres Laufzeitverhaltens und sonstigen Ressourcenverbrauchs bewerten können. Die algorithmische Komplexität von Programmieraufgaben einschätzen können.

Handlungskompetenz

Die Studierenden sollen die wichtigsten, im wirtschaftlichen Umfeld verwendeten Datenstrukturen und Algorithmen kennen, um für vorgegebene Anwendungsfälle geeignete Datenstrukturen und Algorithmen finden, analysieren und bewerten zu können. Überführung von realen Problemstellungen in geeignete, algorithmische Lösungen.

Sozialkompetenz

Die Studierenden sollen sich in einfachen fachlichen Diskussionen über Algorithmen und Datenstrukturen aktiv beteiligen können und z.B. bei der Auswahl einer geeigneten Datenstruktur eine fundierte fachliche Meinung vertreten können. Zudem sollen die Studierenden in der Lage sein, grundlegende Funktionsweisen von einfachen Algorithmen allgemeinverständlich zu erklären.

Inhalt:

- Was sind Algorithmen und Eigenschaften von Algorithmen
- Elementare/grundlegende Datenstrukturen
- Abstrakte Datenstrukturen (Stack, Queue, Bäume, Heap, Hash, …)
- Algorithmische Verfahren (Suche, Sortierung, Rekursion, dynamische Programmierung, …)
- Bewertung von Algorithmen und Datenstrukturen bzgl. Korrektheit, Komplexität, Effizienz und Aufwand

Literatur

- T.H.Cormen, C.E.Leiserson, R.L.Rivest, C.Stein: Algorithmen – Eine Einführung, 4. Aufl., 2013, De Gruyter Oldenbourg
- R. Sedgewick, K. Wayne: Algorithmen: Algorithmen und Datenstrukturen, 2014, Pearson Studium – IT
- G. Saake, K.-W. Sattler: Algorithmen und Datenstrukturen: Eine Einführung mit Java, 5. Aufl., 2013, dpunkt Verlag

Teil II (Fachsemester 3, 4, 5 und 7)

Pflichtmodule (PM)

PM: Wirtschaftsenglisch

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Wirtschaftsenglisch
Modulverantwortliche(r):	Frau Sabine McIntosh, Frau Dr. Martina Zürn
Vorkenntnisse:	Mit Bestehen der jeweiligen Modulprüfung gem. SPO oder Studienplan
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 72 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Vorlesung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Englisch
Leistungsnachweis:	mündliche Prüfung

Qualifikationsziele:

Fach- und Methodenkompetenz:
- Erwerb der Fähigkeit zur flüssigen sozialen Interaktion

Handlungskompetenz:
- Fähigkeit die englische Sprache fach- und berufsbezogen im internationalen Kontext mündlich anzuwenden

Sozialkompetenz:
- Verständnis von interkulturellen Faktoren

Inhalt:
- Ausbau von Grundfertigkeiten
- Einführung in landeskundliche Aspekte des englischen Sprachraumes unter besonderer Berücksichtigung interkultureller Faktoren und Verhaltenskodizes
- Fähigkeit flüssig und angemessen in Bezug auf geschäftliche Situationen zu kommunizieren (Face to Face)
- Erwerb einer Sprechfertigkeit, die es erlaubt ohne Mühe die eigene Meinung klar und angemessen darzulegen (Meeting)
- Fähigkeit schwierige und komplexere Themenstellungen nicht nur zu erfassen, sondern auch zusammenfassend wiederzugeben (Telephoning)
- Übungen zu Textaufbau und Erstellen einer Präsentation
- Graphs und Charts.

Literatur
- Ergänzende Materialien werden über den Overhead-Projektor projiziert bzw. als Handouts verteilt.
- Im Sprachlabor werden Videos und Hörmaterialien eingesetzt.

PM: Technische und organisatorische Datenschutzmaßnahmen

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Technische und organisatorische Datenschutzmaßnahmen
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Module Datenschutzrecht I und Einführung in die IT-Sicherheit
Arbeitsaufwand:	150 Stunden, davon:

	48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:

- Technische Maßnahmen
  - Berechtigungsmanagement / Need-to-know-Prinzip
  - Software-Einsatz
  - Mobile Device Management / VPN
  - Firewall/Antivirus/Back-up
  - Webserver / Mail-Server
  - Patch-Management
- 5.2. Organisatorische Maßnahmen
  - Nachweispflichten
  - Richtlinien
  - Archivierung / Löschung / Entsorgung
  - Auftragsverarbeitung
  - MA-Schulungen

Literatur:

- Peter Münch: Technisch-organisatorischer Datenschutz: - Leitfaden für Praktiker, 4. Auflage (27. April 2010), DATAKONTEXT Verlag, ISBN: 978-3895775864
- Bayerisches Landesamt für Datenschutzaufsicht (Herausgeber), Thomas Kranig, Eugen Ehmann: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket, 1. Auflage (17. November 2017), Verlag C.H.Beck, ISBN: 978-3406716621

PM: Compliance-Management

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Compliance-Management
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Modul Datenschutzrecht I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Sommersemester
Unterrichtsprache:	Deutsch

Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz
Sozialkompetenz

Inhalt:

- Grundelemente des CMS
- Normen (ISO 19600)
- Ermittlung von Compliance-Risiken
- Datenschutzstrukturen / Aufbauorganisation
- Wesentliche Datenschutzprozesse
    - Datenschutzkonforme Datenverarbeitung
    - Sicherstellung der Betroffenenrechte
    - Handhabung von Datenschutzverletzungen
- Dokumentation
- Sensibilisierung der Organisation
- Einbindung in die Corporate Governance

Literatur:

- Kranig T., Sachs, A., Gierschmann, M.: Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag, 2017, ISBN: 978-3846207604
- Detlev Gabel et al.: Rechtshandbuch Cyber-Security: IT-Sicherheit, Datenschutz, Gesellschaftsrecht, M&A, Versicherungen, Compliance, Aufsichtsrecht, Arbeitsrecht, Litigation (Kommunikation & Recht), Deutscher Fachverlag, 1. Auflage (1. Juni 2019), ISBN: 978-3800500123
- KPMG AG WPG: „Das wirksame Compliance-Management-System“, NWB Verlag; 2., vollständig überarbeitete und erweiterte Auflage (6. Januar 2016), 978-3482648526

PM: Web Entwicklung

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Web Entwicklung
Modulverantwortliche(r):	Prof. Dr. Zilker
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Vorlesung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 min)

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden erhalten die Kompetenz einfache Webanwendungen eigenständig zu entwerfen und umzusetzen. Sie sind in der Lage unterschiedlicher Web-Technologien zu verstehen, einzusetzen und in Kombination zu nutzen. Sie erhalten die Kompetenz Inhalte zu strukturieren und plausibel zu verlinken. Weiterhin sind die Studierenden befähigt Inhalte technisch aufzubereiten und in geeigneten Formaten

abzuspeichern. Die Studierenden verfügen über die Fähigkeit einfache 2D-Animationen zu gestalten. Sie verfügen über die Kompetenz komplexere Anwendungssysteme, die auf Content Managementsystemen basieren, individuell hinsichtlich Layouts und Funktionalitäten auszurichten und zu gestalten. **Handlungskompetenz** Die Studierenden erhalten die Kompetenz zielgerichtet Entwicklungswerkzeuge auszuwählen und diese professionell zu nutzen. Sie sind in der Lage statische Web-Anwendungen komplett umzusetzen. Die Studierenden erwerben die Kompetenz komplexe Web-Anwendungen technisch einzuordnen und hinsichtlich einer technischen und gestalterischen Modifikation zu beurteilen.
Inhalt: Begriffsdefinition und generelle Einsatzmöglichkeiten von Multimedia- und Internetanwendungen. Beschreibungssprachen zur Darstellung von Inhalten im Internet (HTML) und Arbeiten mit einschlägigen Entwicklungstools. Darstellung einer Sprache zur Text-, Webseiten- und Bildformatierung, hier Cascading Stylesheets (CSS). Bildbearbeitungssoftware zur Aufbereitung von Bildern für das Web. Grundlegende Techniken zur Bildbearbeitung. Programmiersprachen zur Umsetzung von Funktionalitäten und interaktiven Abfragen auf dem Client, hier JavaScript. Einsatz von Programmierframeworks. Grundlegende Programmierkonzepte dieser Sprache sowie spezifische Eigenschaften und Methoden innerhalb des zugrunde gelegten Objektmodells. Anlegen von bewegten interaktiven Web-Elementen unter Verwendung von einschlägigen Werkzeugen. Aufbau einer, auf einem Content Management System basierenden, Web-Anwendung. Modifikation der bereitgestellten Basisfunktionen durch Programmierung.
Literatur: ● Münz, Gull: HTML Handbuch Franzis Verlag, jeweils neueste Auflage ● Ackermann: JavaScript, Rheinwerk Computing ● Wenz: JavaScript, Galileo Computing, jeweils neueste Auflage ● Laborenz: CSS-Praxis, Galileo Verlag, jeweils neueste Auflage ● Videotutorials laut aktueller Empfehlung ● Webseiten laut aktueller Empfehlung, z.B.: www.selfhtml.org

PM: Privacy Engineering

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Privacy Engineering
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Modul Datenschutzrecht I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Wintersemester
Unterrichtsprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)
In Bearbeitung! **Qualifikationsziele:** **Fach- und Methodenkompetenz** **Handlungskompetenz** **Sozialkompetenz**	
Inhalt:	

- Herkunft: Privacy-by-Design, Privacy Engineer`s Manifesto, Privacy Engineering
- Softwareentwicklung / Softwareeinsatz
- Privacy in der Software-Architektur
- Anonymisierung & Pseudonymisierung
- Löschkonzepte

Literatur:

- Michelle Dennedy, et al.: The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value, Apress Verlag, 1. Auflage (27. Januar 2014), ISBN: 978-1430263555
- Kranig T., Sachs, A., Gierschmann, M.: Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag, 2017, ISBN: 978-3846207604
- Ian Oliver: Privacy Engineering: A Dataflow and Ontological Approach, CreateSpace Independent Publishing Platform; 1. Auflage (18. Juli 2014), ISBN: 978-1497569713
- Aurelia Tamò-Larrieux: Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, Springer Verlag, 1. Auflage 2018 (13. November 2018), ISBN: 978-3319986234
- https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/about

PM: Cloud-Computing

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Cloud-Computing
Modulverantwortliche(r):	Prof. Dr. Jens Söldner
Vorkenntnisse:	Modul Datenschutzrecht I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	6 (4 SU & 2 Ü)
Veranstaltungstyp:	Seminaristischer Unterricht & Übung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:

- Arten des Cloud-Computing: IaaS, PaaS, SaaS
- Private vs. Public Cloud & Hybrid Cloud
- Programmiermodelle, Softwarewerkzeuge und Anwendungen.
- Wirtschaftliche Betrachtungen, Chancen und Risiken des Cloud Computing
- Rechtliche Aspekte, Safe Harbour & Co.
- Entwicklung einfacher Anwendungen in der Cloud

Literatur:

- Wolfgang Tichy, et al.: Cloud Computing (Praxishandbuch), MANZ Verlag Wien, 1. Auflage (10. Januar 2019), ISBN: 978-3214089726
- Karsten Schulz: Datenschutz Cloud-Computing: Ein Handbuch für Praktiker - Leitfaden für IT Management

und Datenschutzbeauftragte, 1. Auflage (4. Mai 2015), epubli Verlag, ISBN: 978-3737544061
- Uwe Irmer: Cloud Security: Band 1 Grundlagen, Books on Demand; Auflage: 1 (27. Juli 2018), ISBN: 978-3752842500
- Brian T. O`Hara: CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide, Sybex; 1. Auflage (14. Juli 2017), ISBN: 978-1119277415

PM: IT-Sicherheitsmanagement

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	IT-Sicherheitsmanagement
Modulverantwortliche(r):	Prof. Dr.-Ing. Sascha Müller-Feuerstein
Vorkenntnisse:	Modul Einführung in die IT-Sicherheit
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:
- Einführung in die ISO/IEC 27001-Familie
- Weitere IT-Sicherheitsmanagementsysteme (ISMS), z.B. BSI Grundschutz, ISIS12
- Einführung, Planung, Betrieb, Verbesserung, PDCA-Zyklus
- Zertifizierung von Personen und Organisationen
- Einbindung in das IT-Servicemanagement & Datenschutzmanagement

Literatur:

- Michael Brenner, et al.: Praxisbuch ISO/IEC 27001 – Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 2. Auflage, neu bearbeitet und erweitert, Hanser Verlag, 2017, ISBN: 978-3446451391
- Thomas W. Harich: IT-Sicherheitsmanagement: Praxiswissen für IT Security Manager, mitp Verlag, 2. Auflage 2018 (30. Juni 2018), 978-3958452732
- Jaqueline Naumann; Ihr Kampf als Informationssicherheitsbeauftragter (ISB) (Die ganze Härte der ISO 27001), Books on Demand Verlag; 2. Auflage (18. September 2018), ISBN: 978-3746091303

PM: Projektmanagement

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Projektmanagement
Modulverantwortliche(r):	Prof. Dr. (UoP) Heesen
Vorkenntnisse:	keine
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des

	Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Vorlesung
Semesterturnus:	Wintersemester
Unterrichtsprache:	Englisch/Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 min)

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden erlernen die wesentlichen Methoden des Projektmanagements, das für die Leitung von Projekten erforderlich ist**.**

Handlungskompetenz
Die Studierenden können mit gängigen Projektmanagementmethoden und -Werkzeugen umgehen.

Inhalt:
Project Management:
- Core functions: Scope Mgmt, Time Mgmt, Cost Mgmt, Quality Mgmt
- Facilitating functions: Human Resources Mgmt, Communication Mgmt, Risk Mgmt, Procurement Mgmt
- Project Integration Management
- Microsoft Project (Anwendung)

Literatur:

- Brewer, J. & Dittman, K. (2009). Methods of IT Project Management. Prentice Hall. ISBN: 0132367254.
- Schwalbe, K. (2009). Information Technology Project Management. Cengage Learning Services. ISBN: 032478855X.
- Marchewka, J. T. (2009). Information Technology Project Management. Wiley. ISBN: 0470409487.

PM: Projekt: DSFA (Folgenab.) mit Risiko

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Projekt: DSFA (Folgenab.) mit Risikomanagement
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Modul Datenschutzrecht I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	6 (4 SU & 2 Ü)
Veranstaltungstyp:	Seminaristischer Unterricht & Übung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fachkompetenz

Methodenkompetenz

Sozialkompetenz

Inhalt:
- Einführung in die Thematik Datenschutzfolgenabschätzung / Privacy Impact Assessments (PIA), Art. 35 DS-GVO

- Datenschutzfolgenabschätzung dem der ISO/IEC 29134
- Risikomanagement dem. ISO 31000 & Einbindung in die DSFA
- Risikoanalyse im Datenschutz (Kurzpapier DSK, Fallbeispiel BayLDA)
- Übung: Fallbeispiel pro Team, Risikoanalyse z.B. Tabellenbasiert

Literatur

- Mathias Reinis: Privacy Impact Assessment: Datenschutz-Folgenabschätzung nach ISO/IEC 29134 und ihre Anwendung im Rahmen der EU-DSGVO (Fit für die EU Datenschutzgrundverordnung 2), Books on Demand Verlag, 2. Auflage (13. Juni 2018), ISBN: -
- BayLDA: Fallstudie Datenschutzfolgenabschätzung, https://www.lda.bayern.de/de/dsfa.html
- DSK-Kurzpapiere: https://www.datenschutzkonferenz-online.de/kurzpapiere.html
- ISO/IEC 29134:2017 Datenschutzfolgenabschätzung: https://www.iso.org/standard/62289.html

PM: Gesetze, Institutionen und Aufgaben

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Gesetze, Institutionen und Aufgaben
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Modul Datenschutzrecht I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:

- Umfassende Behandlung aller mit dem Datenschutz & IT-Sicherheit befassten Institutionen und ihrer Aufgaben/Zuständigkeiten
- Zusammenwirken der Institutionen, insb. auch bei grenzübergreifenden Organisationen
- Institutionen auf Landesebene, z.B.:
  - Landesdatenschutzbehörden (z.B. BayLDA), Landesbeauftragte für Datenschutz (z.B. BayLfD)
  - Landesamt für Sicherheit in der Informationstechnik (LSI)
  - Computer Emergency Response Team (CERT BUND)
- Institutionen auf Bundesebene, z.B.:
  - Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Institutionen auf europ. Ebene, z.B.:
  - Europäischer Datenschutzausschuss (EDSA)
  - European Data Protection Supervisor (EDPS),
  - European Union Agency for Network and Information Security (ENISA)
- Weltweite Zusammenarbeit im Bereich Datenschutz und IT-Sicherheit
- Kirchen, Medien (öff.-rechtl. und privat)

Literatur:
- LayLDA: Zuständigkeiten im Datenschutz: https://www.datenschutz-bayern.de/zustaendigkeiten/
- BfDI: Homepage: https://www.bfdi.bund.de
- THM: Übersicht über DS-Institutionen: https://www.thm.de/datenschutz/en/recht/institutionen.html
- Deutscher CERT-Verbund: https://www.cert-verbund.de/

PM: Unternehmensauditierung

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Unternehmensauditierung
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Modul Datenschutzrecht I
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:
- Ziele von Audits im Allgemeinen und im Bereich IT-Sicherheit und Datenschutz im Speziellen
- Auditplanung, Auditprogramm, Auditdurchführung
- Intern: Rollen, Audittypen, Ablauf eines Audits
- Extern: Prüfpraxis der Aufsichtsbehörden (BayLDA)
- Anforderungen an Auditoren
- Typische Prüffragen

Literatur:
- J. Brauweiler, M. Will, A. Zenker-Hoffmann: Auditierung und Zertifizierung von Managementsystemen: Grundwissen für Praktiker, Springer Gabler, 1. Auflage 2015 (25. August 2015), ISBN: 978-3658102128
- Michael Pachinger: Datenschutz-Audit: Recht - Organisation - Prozess – IT, LexisNexis ARD ORAC Verlag, 2. Auflage aktualisiert (21. Dezember 2017), ISBN: 978-3700770831
- Kranig T., Sachs, A., Gierschmann, M.: Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag, 2017, ISBN: 978-3846207604
- Stefan Beißel: IT-Audit: Grundlagen - Prüfungsprozess - Best Practice, Erich Schmidt Verlag GmbH & Co (18. Februar 2015), ISBN: 978-3503158454

PM: Professionelle Kommunikation

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Professionelle Kommunikation
Modulverantwortliche(r):	Prof. Dr. Hermann
Vorkenntnisse:	keine
Arbeitsaufwand:	150 Stunden, davon:

	48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht & Übung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Mündliche Prüfung (15 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:

- Was bedeutet professionelle Kommunikation?
- Vorbereitung auf den Krisenfall
- Grundzüge der mediale Logik bei Risiken und Krisen, erwartete und unerwartete Auswirkungen
- Wie verhalte ich mich richtig vor der Kamera?
- Souveräne Reaktion auf journalistische Fragestellungen.
- Praktische Übungen vor der Kamera mit Aufnahme und Analyse

Literatur:

- Julia Drews: Risikokommunikation und Krisenkommunikation: Kommunikation von Behörden und die Erwartungen von Journalisten, Springer VS, 1. Auflage 2018 (23. November 2017), ISBN: 978-3658200145
- Jorge Klapproth: Der Tag X - Vorbereitung auf den Ernstfall: Handbuch für Krisenmanagement und Krisenkommunikation, Books on Demand; 4. Auflage (27. September 2018), ISBN: 978-3842332355
- Susanne Fiederer et al.: Effiziente Krisenkommunikation – transparent und authentisch: Mit zahlreichen Praxisbeispielen, Springer Gabler, 1. Aufl. 2017 (1. November 2016), ISBN: 978-3658144197

PM: Big Data Analytics & Statistik

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Big Data Analytics & Statistik
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Selbststudium und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4 (2 SU & 2 Übung)
Veranstaltungstyp:	Seminaristischer Unterricht & Übung
Semesterturnus:	Wintersemester
Unterrichtsprache:	Englisch/Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 Min.)

Qualifikationsziele:

- Organizations across the world are increasingly relying on business analytics and statistics to help them look for latent information revealed through data analysis. An example could be to check the credit worthiness (with objectivity) of an individual using a set of parameters before the issuance of a credit card. Though there could be variations of an individual's parameter from the standard, data analysis and hypotheses testing would reveal whether the difference/deviation is significant.

- At the end of the course, students will be familiar with the use of data analysis and statistics, which can also be beneficial for hypotheses testing (especially useful for research on the bachelor-, master-, and doctoral level) and decision making in real time situations.

Fach- und Methodenkompetenz

Students get to

- Understand the applications of statistical methods in analyzing and interpreting data.
- Understand how to present and display data to convey meaning.
- Prepare and code data for statistical analysis.
- Test hypotheses using statistical tests using statistical software.
- Learn to use the R software and Excel for statistical analyses.

Handlungskompetenz

Students learn to

- Interpret data.
- Derive inferences from the results of statistical tests.
- Make meaningful conclusions from the tested hypotheses.

Sozialkompetenz

Students will know how to

- Model a qualitative statement towards objectivity.
- Select and use the appropriate statistical tests based on the intended objective.

Inhalt:

Big Data

- Origin, volume and format of data
- Business value of Big Data
- Architectures and tools for Big Data Analytics
- Data Analytics Lifecycle
- Discovery
- Data preparation (ETL: extraction, transformation, load)
- Model planning
- Model building
- Communication

Statistics:

- Presenting and displaying data to convey meaning.
- Use the software R and Excel for statistical analysis.
- Framing hypotheses to answer questions.
- Identifying the right statistical method to test hypotheses.
- Coding and preparing data for analysis.
- Interpretation of the results of the statistical tests.

Literatur:

- Heesen, B. (2016). Big Data Analytics: Revolutionizing Strategy Execution (Best Practices for Management). Nuremberg: Prescient Verlag, ISBN: 978-3945156070
- Schmuller, J. (2017). Statistical Analysis with R for Dummies. Hoboken, New Jersey: John Wiley & Sons. ISBN: 978-1-119-33706-5 or 978-1-119-33726-3

FWPM: Datenschutz und IT-Sicherheit bei BYOD

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Datenschutz und IT-Sicherheit bei BYOD
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	-
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:

- Einbindung von Mobilgeräten in die IT-Governance
- Mobile Device Management Systeme
- Systematische Anpassung der Prozesse im Unternehmen
- Schwachstellen, Risikoanalyse und notwendige Sicherheitsmaßnahmen
- DS-rechtliche Aspekte bei der Vermischung privater und geschäftlicher Daten auf einem Mobilgerät

Literatur:

- Wolf Knüpffer et al.: Integration mobiler IT-Systeme: Einsatzfelder - Management – Strategie, Erich Schmidt Verlag GmbH & Co (21. Februar 2017), ISBN: 978-3503171569
- Christine Monsch: Bring Your Own Device (BYOD).: Rechtsfragen der dienstlichen Nutzung arbeitnehmereigener mobiler Endgeräte im Unternehmen. (Schriften zum Sozial- und Arbeitsrecht), Duncker & Humblot Verlag, 1. Auflage (1. Juni 2017), ISBN: 978-3428150168
- Andreas Kohne et al.: Bring your own Device: Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen, Risiken und Möglichkeiten, Springer Vieweg Verlag, 1. Auflage 2015 (11. September 2015), ISBN: 978-3658037161
- Heinrich Kersten et al.: Mobile IT-Infrastrukturen: Management, Sicherheit und Compliance, mitp Verlags GmbH & Co. KG; 1. Auflage 2014 (20. Dezember 2014), ISBN: 978-3826697159

Wahlpflichtmodule (WPM)

WPM: Softwareentwicklung für Mobilgeräte

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Softwareentwicklung für Mobilgeräte
Modulverantwortliche(r):	Prof. Dr. Wolf Knüpffer, Prof. Dr. Michael Zilker, Prof. Dr.-Ing. Sascha Müller-Feuerstein
Vorkenntnisse:	-
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Selbststudium und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Seminaristischer Unterricht und Übung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Studienarbeit

Qualifikationsziele:

Fach- und Methodenkompetenz
Der Studierende erhält die Kompetenz Apps für mehrere Plattformen zu planen und mit den jeweiligen Softwareentwicklungstools zu programmieren und zu produzieren. Dabei erweitert der Studierende seine Kompetenz spezifische App Technologien auszuwählen und in einem konkreten Projekt zu implementieren. Sie werden befähigt geeignete Entwicklungswerkzeuge auszuwählen und anzuwenden.

Handlungskompetenz
Die Studierenden vertiefen die Kompetenz mit mehreren spezifischen Entwicklungstools umzugehen und unter Verwendung einer Programmier- und Beschreibungssprachen Funktionalitäten und Interaktionen programmieren. Sie sind in der Lage eigenständige Apps zu gestalten und technisch umzusetzen.

Sozialkompetenz
Die Studierenden vertiefen die Kompetenz sich in Projektteams zu integrieren. Sie erwerben, die im späteren Berufsleben geforderte, Kommunikationsfähigkeit und sind befähigt sich in einem Team zu positionieren.

Inhalt:

- Spezifische App-Technologien, wie z.B. Sensoren, Touchscreen, Navigation mit Gesten, Kamerafunktion, Stromsparmechanismen
- Grundlagentechnologien für die App-Entwicklung, wie z.B. Datenbanken, Http-Requests, Cloudanbindung, Webservices, Broadcast-Messaging-Systeme
- Bearbeitung eines Entwicklungs-Projektes mit 2 von 3 Plattformen (Android, iOS und Windows)

Literatur:

- Gargenta, Marko; Nakamura, Masumi: Learning Android: Develop Mobile Apps Using Java and Eclipse, 2nd edition, 2014, ISBN: 978-1449319236
- Künneth, Thomas: Android 7: Das Praxisbuch für Entwickler, Rheinwerk Computing, 4. Auflage, 2016, ISBN: 978-3836242004
- Petzlod, Charles: Creating Mobile Apps with Xamarin.Forms, Microsoft Press, 1. Auflage, 2015, eBook
- Huber, Thomas Claudius: Windows Store Apps mit XAML und C#, Galileo Computing, 1. Auflage, 2013, ISBN: 978-3836219686
- Knüpffer, W. (Hrsg). et al.: Integration mobiler IT-Systeme; Einsatzfelder - Management – Strategie, Erich Schmidt Verlag, 2017, ISBN: 978-3-503-17156-9.
- Kofler, M.: Swift 4: Das umfassende Praxisbuch. Apps entwickeln für iOS, macOS und Apple TV. Ideal für Umsteiger von Objective-C, Rheinwerk Computing, 2017. ISBN: 978-3836259200.

WPM: Soft Skills – Training

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Soft Skills - Training
Modulverantwortliche(r):	Prof. Dr. Schön, Herr Dr. Endres (LB, Moduldurchführender)
Vorkenntnisse:	keine, max. 20 Teilnehmer
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Vorlesung
Semesterturnus:	Jedes Semester, Blockveranstaltung
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Studienarbeit

Qualifikationsziele:

Herausforderungen im Arbeitsalltag meistern:

- Stärkung der Selbstverantwortung
- Bewusstwerdung des eigenen Verhaltens und deren Hintergründe
- Erkennen anderer Verhaltensmöglichkeiten
- Verhalten in Konflikten, Umgehen mit schwierigen Situationen
- Teamfähigkeit
- Ergebnisorientierung im Team
- Erreichen des eigenen Bestzustands durch Fokussierung auf die eigenen Ressourcen
- Besseres Selbstmanagement

Inhalt:

Einführung und Kennenlernen (ca. ½ Tag):

- Womit bin ich hier, was beschäftigt mich?
- Was verstehen wir unter „Soft Skills“?
- Warum bin ich hier, was möchte ich erreichen?

Teamarbeit im Projekt (ca. 1 Tag):

Projekt in parallelen Teams (incl. Stress-Erfahrung) mit Vorlagen, Rollen, Präsentation und Bewertung

- Erleben und Bewusstwerdung des eigenen Rollen- und Stressverhaltens
- Was macht ein Team aus? Entwicklung und Reifegrad von Teams, ...
- Negative und positive Teammuster – gespiegelt an den Projekterfahrungen
- Erfolgsfaktoren von Teams – gemäß aktuellen Erfahrungen
- Feedback der Teammitglieder untereinander

Ressourcen (ca. ½ Tag):

- Was mich zum Strahlen bringt, meine Leidenschaft
- Was treibt mich an?

Stress, Konflikte, Belastungen, … (ca. ½ Tag):

- Was löst bei mir Stress aus, welche Situationen erlebe ich als schwierig, belastend?
- Mein „Antityp“ und wie ich mit ihm umgehe – Übung mit Präsentation und Feedback
- Emotionen in schwierigen Situationen: automatische Reaktionen als Weckrufe

Umgehen mit schwierigen Situationen (ca. 1½ Tage):

- Meine Erfahrung mit Konflikten, Stress, etc., mein Umgang damit
- Übung „Fliegende Eier“ – Stress und Kommunikationshindernisse in Echtzeit

- Wie Konflikte entstehen und eskalieren
- De-Eskalation und innere Haltung
- Kommunikation – was ich sagen will und was ankommt
- Auf welchem (der 4) Ohren höre ich wie gut?
- Von Annahmen zu anderen Blickwinkeln – trotz Enttäuschung „am Boden bleiben“

Bestzustand (ca. ½ Tag):
- Stimmig mit meinem Herzenswunsch? Motive und Motivation
- Welche Aufgabe, Rolle ist mir auf den Leib geschneidert
- Was bringt mich in meinen Bestzustand? Wie nutze ich meine Ressourcen / Erfolgserlebnisse optimal?

Umsetzung (ca. ½ Tag):
- Was nehme ich mit, was will ich wie umsetzen?
- Feedback der Teilnehmer untereinander und an den Trainer
- Persönliches Feedback, Coaching (auf Wunsch)

WPM: Softwarequalitäten von Java Projekten in der Praxis

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Softwarequalitäten von Java Projekten in der Praxis
Modulverantwortliche(r):	Prof. Dr. Schön (Modulverantwortlicher), Herr Hock (LB, Moduldurchführender)
Vorkenntnisse:	Mit Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan,
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Vorlesung
Semesterturnus:	Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 min)

Qualifikationsziele:
Die Studierenden erwerben vertiefte Kenntnisse und Fähigkeiten zur Analyse, Beurteilung und Verbesserung von Software-Qualität. Sie sind in der Lage Prinzipien, Patterns, Techniken und Tools, die zum Schreiben von sauberem Code benötigt werden, anzuwenden.

Inhalt:
Die Prüfung von Software ist nicht auf eine bestimmte Phase im Projekt beschränkt. Schon während der Coding-Phase bzw. des System-Build-Prozesses können kritische und schwierig zu findende Softwaredefekte im Quellcode aufgedeckt werden. In der Vorlesung werden die dafür nötigen Verfahren und Tools vorgestellt. Unter anderem werden die folgenden Themen behandelt:

- Übersicht über die Grundlagen der Software-Qualität
- Softwaremetriken, Metrikanwendung in der Praxis
- Überblick über Prinzipien, Best Practices und Code Smells
- Einhaltung und Überprüfung Java Code Conventions
- Statische Softwareprüfung, insbesondere Review-Techniken und statische Programmanalyse
- Sicherung der Softwarequalität mit Werkzeugen wie SonarQube, PMD, FindBugs und Checkstyle
- Softwaretests mit JUnit
- Überprüfen der Testabdeckung (Code Coverage)
- Continuous Integration

• Design Prinzipien • Design Patterns (GoF)
Literatur: • Die Studierenden können mit gängigen Projektmanagementmethoden und -werkzeugen umgehen. • Schneider, Kurt: Abenteuer Software Qualität – Grundlagen und Verfahren für Qualitätssicherung und Qualitätsmanagement, dpunkt.verlag, 2007 • Robert, Martin: Clean Code – Refactoring, Patterns, Testen und Techniken für sauberen Code, mitp-Verlag, 2009 • Lilienthal, Carola: Langlebige Software-Architekturen, Dpunkt Verlag, 2015 • Bloch, Joshua: Effective Java – Second Edition, Addision Wesley, 2008 • Roock, Stefan: Refactorings in grossen Softwareprojekten, Dpunkt Verlag, 2004 • Gamma, Erich: Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley Professional, 1994 • Robert C. Martin: Agile Software Development: Principles, Patterns and Practices, Prentice Hall, 2003

Spezialisierungsmodule (SPM)

IT-Forensik

SPM: IT-Forensik: Forensische Datenalayse

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	IT-Forensik: Forensische Datenanalyse
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Keine
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Sommersemester
Unterrichtsprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz
Sozialkompetenz

Inhalt:

- Einführung in die IT-Forensik, Motivation, Bedrohungssituationen
- Incident Response
- Vorgehensmodell im Verdachtsfall:
  - Identifikation
  - Datensicherung
  - Analyse
  - Dokumentation und Aufbereitung
- Rückverfolgung von Spuren in Netzwerken
- Aspekte des Datenschutzes bei der forensischen Analyse
- Kooperation mit Behörden und Sicherheitseinrichtungen, Beweissicherung

Literatur:

- Andreas Dewald, et al.: Forensische Informatik (German Edition), Books On Demand Verlag (October 28, 2015), ISBN: 978-3842379473
- Stefan Meier: Digitale Forensik in Unternehmen, Dissertation, https://epub.uni-regensburg.de/35027/1/Dissertation_Veroeffentlichung_Stefan_Meier_A5_digital.pdf
- André Arnes: Digital Forensics, Wiley Verlag; 1. Auflage ((July 24, 2017), ISBN: 978-1119262381
- Alexander Geschonneck: Computer-Forensik (iX Edition): Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag GmbH; 6. Auflage, akt. u. erw. Aufl. (3. April 2014), ISBN: 978-3864901331
- Timo Steffens: Auf der Spur der Hacker: Wie man die Täter hinter der Computer-Spionage enttarnt, Springer Vieweg Verlag, 1. Auflage 2018 (15. Februar 2018), ISBN: 978-3662559536
- BSI: Leitfaden IT-Forensik, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html

SPM: IT-Forensik: Forensik-Praktikum

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	IT-Forensik: Forensik-Praktikum
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Keine
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Übung
Semesterturnus:	Sommersemester
Unterrichtsprache:	Deutsch
Leistungsnachweis:	Mündliche Prüfung am System (20 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz
Sozialkompetenz

Inhalt:

- Durchführung praktischer Übungen der IT-Forensik an Beispielszenarien in virtuellen Umgebungen
- Einsatz verschiedener Tool-Sets zur Durchführung und Einübung forensischer Vorgehensweisen, Z.B. CAINE, EnCase, Sleuth Kit, etc.
- Übung in ausgewählten BS-Umgebungen (insb. Dateinsysteme) und mit verschiedenen Speichermedien

Literatur:

- Bruce Nikkel: Practical Forensic Imaging: Securing Digital Evidence with Linux Tools, No Starch Press, 1. Auflage (1. September 2016), ISBN: 978-1593277932
- Harlan Carvey: Investigating Windows Systems: Academic Press; 1 edition (August 30, 2018), ISBN: 978-0128114155
- Lee Reiber: Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation, McGraw-Hill Education; 2 edition (January 3, 2019), ISBN: 978-1260135091
- Suzanne Widup: Computer Forensics and Digital Investigation with EnCase Forensic v7, McGraw-Hill Education; 1 edition (May 28, 2014), ISBN: 978-0071807913

Netzwerksicherheit

SPM: Netzwerksicherheit: Analyse

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Netzwerksicherheit: Analyse
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	keine
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4 (2SU & 2Ü)
Veranstaltungstyp:	Seminaristischer Unterricht & Übung
Semesterturnus:	Sommersemester

Unterrichtssprache:	Deutsch
Leistungsnachweis:	Mündliche Prüfung (20 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:

- Vertiefte Grundlagen von Netzwerkprotokollen, insb. TCP/IP
- Analyse von Netzwerktopologien, Auffinden von Schwachstellen
- Analyse von Netzwerkprotokollen, Identifikation von Schwachstellen
- Absicherung von Netzwerken / Netzwerkprotokollen
- Vertiefung und Veranschaulichung der behandelten Themen in der Übung

Literatur:

- James Forshaw: Netzwerkprotokolle hacken: Sicherheitslücken verstehen, analysieren und schützen, dpunkt.verlag GmbH, 1. Auflage (25. Juni 2018), ISBN: 978-3864905698
- Laura Chappel: Wireshark® 101: Einführung in die Protokollanalyse, mitp Verlag, 2. Auflage 2018 (31. Januar 2018), ISBN: 978-3958456839
- Tim Philipp Schäfers: WLAN Hacking: Schwachstellen aufspüren, Angriffsmethoden kennen und das eigene Funknetz vor Hackern schützen. WLAN-Grundlagen und Verschlüsselungsmethoden erklärt, FRANZIS Verlag GmbH, 1. Auflage (15. Januar 2018), ISBN: 978-3645605236
- Steffen Wendzel: IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung, Springer Vieweg Verlag,1. Auflage 2018 (5. September 2018), ISBN: 978-3658226022
- Eric D. Knapp et al.: Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Syngress Verlag, 2. Auflage (15. Dezember 2014), ISBN: 978-0124201149

SPM: Netzwerksicherheit: Client & Server

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Netzwerksicherheit: Client & Server
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	keine
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4 (2SU & 2Ü)
Veranstaltungstyp:	Seminaristischer Unterricht & Übung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Mündliche Prüfung (20 Min.)

In Bearbeitung!

Qualifikationsziele:

Handlungskompetenz

Fach- und Methodenkompetenz

Sozialkompetenz

Inhalt:

- Absicherung von Client- & Serversystemen (insb. Windows & Linux)
- Grundlagen Public Key Infrastruktur (PKI) & Zertifikate
- Richtige Konfiguration von Firewalls, Einrichtung von VPNs
- Verschlüsselung der Dateiablage, z:B. Bitlocker, True-/VeraCrypt, etc.
- Intrusion Detection & Prevention Systeme, z.B. Snort, OSSEC, Security Onion, etc.
- Honey Pots & Co.
- DevOps zur Institutionalisierung sicherer AbläufeN

Literatur:

- Peter Kloep: PKI und CA in Windows-Netzwerken: Das Handbuch für Administratoren. Zertifikat-Management und Sicherheit für Ihre Windows-Systeme, Rheinwerk Computing, 1. Auflage (27. Dezember 2017), ISBN: 978-3836255905
- Donald A. Tevault: Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats, Packt Publishing - ebooks Account (January 11, 2018), ISBN: 978-1788620307
- Kyle Rankin: Linux Hardening in Hostile Networks: Server Security from TLS to Tor, Addison-Wesley Professional, 1 edition (August 5, 2017), ISBN: 978-0134173269

IT-Infrastruktur

SPM: IT-Infrastruktur: IT-Servicemanagement

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	IT-Servicemanagement
Modulverantwortliche(r):	Prof. Dr.-Ing. Sascha Müller-Feuerstein
Vorkenntnisse:	-
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Selbststudium und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Seminaristischer Unterricht und Übung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (90 Min.)

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden verfügen über ein umfassendes Basiswissen im Bereich IT-Servicemanagement (ITSM). Neben den Grundkonzepten des ITSM kennen Sie die wichtigsten Prozesse, Rollen und Problembereiche des Betriebs mittlerer bis großer IT-Infrastrukturen.

Handlungskompetenz
Die Studierenden verfügen über die Fähigkeit typische Problem mittlerer und großer IT-Betriebe zu erkennen und durch den Einsatz von Best-Practice-Methoden im Bereich ITSM gezielt auf deren Lösung hinzuwirken.

Sozialkompetenz
Die Studierenden können sowohl mit IT-Fachleuten, als auch mit Fachanwendern effektiv und situationsgerecht kommunizieren. Sie sind geübt in der Zusammenarbeit in kleinen bis mittleren Teams und kennen grundlegende Strategien der Arbeitsteilung.

Inhalt:
Umfassender Einblick in die wichtigsten IT-Servicemanagementprozesse eines IT-Betriebs, basierend auf dem IT-Best-Practice-Rahmenwerk IT Infrastructure Library (ITIL). Am Rande werden zudem ISO 20k, CoBIT und ISO 27001 behandelt. Neben den Prozessdefinitionen werden u.a. die kritischen Erfolgsfaktoren, Rollen, Kennzahlen

und Schnittstellen der ITIL-Kernprozesse im Detail behandelt und durch Fallstudien weiter vertieft. Optional ist die Teilnahme an einer zusätzlichen und kostenpflichtigen ITIL-Foundation-Zertifizierungsprüfung möglich.
Literatur: ● Böttcher, Roland: IT-Service-Management mit ITIL® - 2011 Edition: Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen. Heise Verlag, 3. Auflage, 2012, ISBN: 978-3936931808 ● Van Bon, Jan: Itil® 2011 Edition – Das Taschenbuch. Van Haren Publishing, 2012. ISBN: 978-9087537050 ● Nadin Ebel: Basiswissen ITIL® 2011 Edition: Grundlagen und Know-how für das IT Service Management und die ITIL®-Foundation-Prüfung. dpunkt.verlag GmbH; 1. Auflage, 2014. ISBN: 978-3864901478.

SPM: IT-Infrastruktur: IT-Planung und Administration

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	IT-Planung und Administration
Modulverantwortliche(r):	Prof. Dr. Jens Söldner
Vorkenntnisse:	-
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Selbststudium und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Seminaristischer Unterricht und Übung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Prüfung am System (20 Min.)

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden verfügen über detaillierte Kenntnisse der typischen administrativen Aufgaben und Abläufe, die im Kontext des Betriebs eines modernen Betriebssystems anfallen. Weiterhin verfügen die Studierenden über ein Grundverständnis bzgl. der Zusammenhänge und Abläufe innerhalb eines modernen Betriebssystems. Die Studierenden können grundlegende Zusammenhänge zwischen administrativen Tätigkeiten und dem Management des IT-Betriebs erkennen.

Handlungskompetenz
Die Studierenden können die administrativen Kernaufgaben der Einrichtung und Administration eines modernen Betriebssystems in typischen Einsatzszenarien selbstständig durchführen. Weiterhin können die Studierenden aktiv an der Planung, Realisierung und Leitung eines IT-Betriebs teilnehmen.

Sozialkompetenz
Die Studierenden können sowohl mit IT-Fachleuten, als auch mit Fachanwendern effektiv und situationsgerecht kommunizieren. Sie sind geübt in der Zusammenarbeit in kleinen bis mittleren Teams und kennen grundlegende Strategien der Arbeitsteilung.

Inhalt:
Vermittlung der typischen Administrations- und Planungsaufgaben für den Betrieb eines modernen Betriebssystems und Vertiefung der Lehrinhalte durch praktische Übungen am Rechner. Behandlung von grundlegenden Planungsstrategien für mittlere bis große Netzwerkinstallationen und Vertiefung der Lehrinhalte durch Fachdiskussionen auf Basis von typischen Beispielszenarien.

Literatur:
- Microsoft Corp.: 21410B: Installieren und Konfigurieren von Windows Server 2012 (Kursunterlagen, MS IT-Academy)
- Joos, Thomas: Microsoft Windows Server 2016 - Das Handbuch: Von der Planung und Migration bis zur Konfiguration und Verwaltung. O'Reilly Verlag, 1. Auflage 2017, ISBN: 978-3960090182

Datenschutzmanagement

SPM: Datenschutzmanagement: Implementierung

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Datenschutzmanagement: Implementierung
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	-
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Selbststudium und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Seminaristischer Unterricht und Übung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz
Sozialkompetenz

Inhalt:

- Vorgehen bei der Implementierung einer DS-GVO-konformen Organisation
- Schaffung von DS-Awareness bei MitarbeiterInnen
- Schulungskonzepte im mittleren bis größeren Organisationen
- Implementierung eines DSMS: Vorgehensmodelle, kritische Punkte und Herausforderungen, Risikomanagement
- Vorbereitung auf Akkreditierung und Prüfungen von Behörden

Literatur:

- Lukas Feiler et al.: Umsetzung der DSGVO in der Praxis: Fragen, Antworten, Muster, Verlag Österreich (1. Februar 2018), ISBN: 978-3704678591
- DIN e.V. et al.: Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung: Lösungen zur praktischen Umsetzung Textbeispiele, Musterformulare, Checklisten, Beuth; Auflage: vollständig überarbeitete und erweiterte (24. Mai 2018), ISBN: 978-3410279815
- Patrick M. Petzka: DSGVO - Lehr- und Arbeitsbuch zur Mitarbeiterunterweisung/-schulung anhand der Datenschutzgrundverordnung DSGVO und des Bundesdatenschutzgesetz BDSG, Petzka Verlag (Nova MD), Erstauflage (14. Dezember 2018), ISBN: 978-3961118090
- Bernhard Bauer-Banzhaf: Die Fundstelle: Sonderheft: Die Umsetzung der Datenschutz-Grundverordnung (DSGVO) in den Kommunen, Richard Boorberg Verlag, 1. Auflage (5. Juni 2018), ISBN: 978-3415063327

SPM: Datenschutzmanagement: Praktikum

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Datenschutzmanagement: Praktikum
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	-
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Selbststudium

	und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Übung und Seminaristischer Unterricht
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Mündliche Prüfung (20 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach- und Methodenkompetenz

Handlungskompetenz
Sozialkompetenz

Inhalt:

- Durchführung einer umfassenden Fallstudie im Kontext Datenschutzmanagement
- Falls möglich Einbindung von regionalen Unternehmen und Organisationen zur Sicherstellung möglichst praxisnaher Fragestellungen
- Die Studierenden sollten das im SPM: Datenschutzmanagement: Implementierung gewonnene Wissen möglichst unmittelbar in die Praxis umsetzen können

Literatur:

- Markus Schäffter: Datenschutzmanagement 2.0: EU-konformen Datenschutz effizient planen und umsetzen, CreateSpace Independent Publishing Platform (7. Oktober 2017), ISBN: 978-1976387388
- BayLDA: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket, C.H.Beck Verlag, 1. Auflage (17. November 2017), ISBN: 978-3406716621

Vertiefung oder Erweiterung der Spezialisierung (VESPM)

VESPM: IT-Forensik

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	IT-Forensik: Hardware-Forensik
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Keine
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	Seminaristischer Unterricht
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung!

Qualifikationsziele:

Fach und Methodenkompetenz

Handlungskompetenz

Sozialkompetenz

Inhalt:

- Grundlagen der HW-Forensik, Basis für die weiteren Analysen
- Aufrechterhaltung von Beweisketten, Datenflüchtigkeit
- Datensicherung mit Hilfe von Forensische Duplikate, z.B. mit dd_rescue und HW-Writeblocker
- Einsatz von Prüfsummen zur Verifizierung der Echtheit
- Umgang mit laufenden, verschlüsselten Systemen
- Hardware-Tools und Medien der HW-Forensik, insb. auch für Mobilgeräte

Literatur:

- Bruce Nikkel: Practical Forensic Imaging: Securing Digital Evidence with Linux Tools, No Starch Press, 1. Auflage (1. September 2016), ISBN: 978-1593277932
- Michael Hale Ligh et al.: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, WileyVerlag, 1 edition (July 28, 2014), ISBN: 978-1118825099

VESPM: Netzwerksicherheit: Hacking

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Netzwerksicherheit: Hacking
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Keine
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4 (2SU + & 2Ü)
Veranstaltungstyp:	Seminaristischer Unterricht & Übung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Mündliche Prüfung (20 Min.)

In Bearbeitung! **Qualifikationsziele:** **Fach- und Methodenkompetenz** **Handlungskompetenz** **Sozialkompetenz**
Inhalt: • Passwort-Hacking: Brute-Force, Rainbow-Tables • Penetration-Testing & Firewalls: Stateless, Next-Generation Firewalls • Hacking-Tools, z.B. KaLi-Linux, Metasploit • Netzwerkverkehrsanalyse mit Wireshark & Co. • Systemüberwachung mit Nagios • Social Engineering & Der Faktor Mensch beim Hacking • Praktische Übungen mit den vorgestellten Tools in virtueller Umgebung
Literatur: • Michael Messner: Hacking mit Metasploit: Das umfassende Handbuch zu Penetration Testing und Metasploit, dpunkt.verlag GmbH; 3. Auflage, akt. u. erw. (30. Oktober 2017), ISBN: 978-3864905230 • Peter Kim: The Hacker Playbook 3: Practical Guide To Penetration Testing, Independently published (2. Mai 2018), ISBN: 978-1980901754 • Mark B.: Hacken mit Kali-Linux: Schnelleinstieg für Anfänger, Books on Demand Verlag, 1. Auflage: (1. November 2017), ISBN: 978-3746012650 • Christopher Hadnagy: Die Kunst des Human Hacking, mitp-Verlag; Auflage: 2011 (25. Oktober 2011), ISBN: 978-3826691676 • Kevin D. Mitnick et al.: Die Kunst der Täuschung: Risikofaktor Mensch, MITP; Sonderausgabe (27. März 2006), ISBN: 978-3826615696

VESPM: IT-Infrastruktur: IT-Collaboration und Integration

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	IT-Collaboration und Integration
Modulverantwortliche(r):	Prof. Dr.-Ing. Sascha Müller-Feuerstein & Prof. Dr. Jens Söldner
Vorkenntnisse:	-
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Selbststudium und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Seminaristischer Unterricht und Übung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Prüfung am System (20 Min.)

Qualifikationsziele:

Fach- und Methodenkompetenz

Die Studierenden kennen die typischen Anforderungen an Lösungen zur IT-Collaboration und die damit einhergehenden datenschutzrechtlichen und sicherheitstechnischen Fragestellungen in kleinerer bis mittlerer Unternehmen. Die Studierenden haben erste praktische Erfahrungen mit der Einrichtung, Konfiguration und dem Betrieb einer modernen Software zur Unterstützung von Arbeitsabläufen in Teams gesammelt. Die Studierenden kennen die wichtigsten datenschutzrechtlichen Rahmenbedingungen, sowie technische Grundlagen für die Sicherstellung des technischen Datenschutzes kleinerer bis mittlerer Organisationen.

Handlungskompetenz
Die Studierenden können im Unternehmen aktiv an der Entwicklung einer IT-gestützten Collaborationlösung mitarbeiten. Sie besitzen die Fähigkeit eine moderne IT-Collaboration-Software in kleinen bis mittleren Unternehmen, insb. auch unter datenschutzbezogenen Aspekten, zu planen, einzurichten und zu betreiben. Die Studierenden sind fähig an Konzeption und Aufbau einer sicheren Netzwerk- und Systeminfrastruktur aktiv mitzuwirken und einfache Konfigurationsaufgaben selbständig zu übernehmen.

Sozialkompetenz
Die Studierenden sind in der Lage die Vorteile der IT-Unterstützung von Arbeitsabläufen typischer Information-Worker zu vermitteln und können die Anwender schrittweise an dieses neue Werkzeug heranführen. Die Studierenden können Anwendern verständlich vermitteln warum bestimmte technische, organisatorische und datenschutzrechtliche Maßnahmen notwendig sind, um die IT-Sicherheit im Unternehmen zu gewährleisten.

Inhalt:
Die Lehrveranstaltung ist eine Kombination zweier eigenständiger Teile, die in der Praxis oft Hand in Hand gehen: Die Unterstützung der Zusammenarbeit von Information-Workern im Unternehmen und der sichere Aufbau und Betrieb von Netzwerken in kleineren bis mittleren Organisationen. Unter anderem werden die folgenden Themen behandelt:

- Web Content Management (WCM) / Records Management
- Workflow Management (WfM)/ Business Process Management (BPM)
- Document Management (DM)
- Microsoft SharePoint Online und SharePoint Server
- Ausgewählte Grundlagen des Datenschutzrechts und rechtliche Anforderungen an Unternehmen
- Einsatz von Cloud-Computing und cloud-basierten Lösungen zur Förderung der IT-Collaboration
- Sicherheitsaspekte von Netzwerkinfrastrukturen und ausgewählte Angriffsvektoren

Literatur:

- Lanphier, Troy: "Managing Microsoft SharePoint Server 2016 ", Microsoft Press, 2016, ISBN: 978-1509302949
- Andrew S. Tanenbaum; David J. Wetherall: "Computernetzwerke", Pearson Studium, 5. Auflage, 2012, ISBN: 978-3866451568
- Kranig, Thomas; Sachs, Andreas; Gierschmann, Markus: Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden, Bundesanzeiger; 1. Auflage, 2017, ISBN: 978-3846207604
- Petrlic, Ronald, et al.: "Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie", Springer Vieweg; 1. Auflage, 2017, ISBN: 978-3658168384

VESPM: Datenschutzmanagement

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Datenschutzmanagement: Governance und rechtliche Rahmenbedingungen
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	-
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Selbststudium und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Seminaristischer Unterricht und Übung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Prüfung (60 Min.)

In Bearbeitung! **Qualifikationsziele:** **Fach- und Methodenkompetenz** **Handlungskompetenz** **Sozialkompetenz**
Inhalt: • Datenschutz in das Business-IT-Alignment einbeziehen. • Einbindung des DSMS in die Unternehmens-Governance • Rechtliche Rahmenbedingungen, die über die Datenschutzrechtlichen Aspekte hinaus gehen (Mitbestimmung, Betriebsrat, etc.) • Verknüpfung mit dem IT-Management, IT-Servicemanagement, IT-Sicherheitsmanagement, Katastrophenmanagement, etc. • Verknüpfung mit der internen IT-Revision
Literatur: • Matthias Knoll et al.: IT-GRC-Management – Governance, Risk und Compliance: Grundlagen und Anwendungen (Edition HMD), Springer Vieweg, 1. Auflage 2017 (29. Januar 2018), ISBN: 978-3658200589 • Inge Hanschke: Informationssicherheit & Datenschutz – einfach & effektiv: Integriertes Managementinstrumentarium systematisch aufbauen und verankern, Carl Hanser Verlag GmbH & Co. KG (9. September 2019), ISBN: 978-3446458185 • Aleksandra Sowa et al.: IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die IT-Prüfung, Springer Vieweg; 2. Auflage, aktual. Aufl. 2019 (4. Mai 2019), ISBN: 978-3658237646

Bachelorarbeit (Bar)

BAr: Bachelorseminar

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Bachelorseminar
Modulverantwortliche(r):	Professoren des Bachelorstudienganges Datenschutz und IT-Sicherheit
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	90 Stunden, davon: 24 Stunden Präsenzzeit, 66 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	3
Semesterwochenstunden:	2
Veranstaltungstyp:	Seminar
Semesterturnus:	Sommer- und Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Teilnahme und Referat

Qualifikationsziele:

Handlungskompetenz
Die Studierenden erhalten die Kompetenz den Hergang ihre Bachelorarbeit in unterschiedliche Entwicklungsstufen zu beleuchten und wissenschaftlich darzustellen.

Sozialkompetenz
Die Teilnehmer erlangen weiterhin die Kompetenz ihre Arbeit fachlich fundiert in einem studentischen Plenum zu präsentieren und zu verteidigen.

Inhalt:
- Präsentation von Zwischen- und Endergebnissen

• Diskussion von Thesen • Diskussion von Ergebnissen • Fortentwicklung von wissenschaftlichen Arbeiten • Wissenschaftliches Arbeiten

BAr: Bachelorarbeit

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Bachelorarbeit
Modulverantwortliche(r):	Professoren des Bachelorstudienganges Datenschutz und IT-Sicherheit
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	360 Stunden
ECTS-Punkte:	12
Semesterwochenstunden:	-
Veranstaltungstyp:	Wissenschaftliche Arbeit
Semesterturnus:	Sommer- und Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Schriftliche Arbeit
Qualifikationsziele: **Handlungskompetenz** Befähigung zur Anfertigung einer wissenschaftlichen Arbeit basierend auf einem praktischen Projekt. Hinführen zum selbstständigen wissenschaftlichen Arbeiten. Die Teilnehmer erlangen die Kompetenz eine wissenschaftliche Fragestellung in einer Arbeit zu strukturieren und textlich auszuformulieren und die Ergebnisse der Arbeit adäquat zu diskutieren.	
Inhalt: Das Thema der Bachelorarbeit wird individuell aus dem Bereich des Themengebietes des Datenschutzes und der IT-Sicherheit gewählt. Die theoretische Arbeit wird auf der Grundlage eines praktischen Projektes formuliert und zeigt die aktuellen Fragestellungen des gewählten Themas sowie deren Lösungsansätze und -wege im Kontext des Projektes auf.	
Literatur: ● Heesen, Wissenschaftliche Arbeiten schreiben mit Word 2016, Prescient Verlag, 2016	

Teil III (6.Fachsemester)

Praktisches Studiensemester (prS)

prS: Betriebliche Praxis

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Betriebliche Praxis
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	540 Stunden 20 Wochen Präsenzzeit in einer Unternehmung oder Organisation.
ECTS-Punkte:	18
Semesterwochenstunden:	
Veranstaltungstyp:	Praktikum
Semesterturnus:	Sommer- und Wintersemester

Unterrichtssprache:	Deutsch
Leistungsnachweis:	Abgabe der entsprechenden Unterlagen (Praktikumsvertrag, Praktikumszeugnis)

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden erwerben im Praktikum individuelle Fachkenntnisse aus dem jeweils anstehenden Aufgabenfeld. Thematisch sollte die, im Studium erworbene Fachkompetenz, durch konkrete betriebliche Tätigkeiten gefestigt und erweitert werden.

Handlungskompetenz
Die Studierenden erwerben die Kompetenz Aufgaben aus der betrieblichen Praxis des Datenschutz und der IT-Sicherheit zu übernehmen und zu bearbeiten. Dabei erwerben sie die Fähigkeit Entscheidung im gesetzten Rahmen zu treffen und zu verantworten

Sozialkompetenz
Die Studierenden erwerben die Kompetenz im betrieblichen Team zu arbeiten. Dabei erlangen sie die Fähigkeit eigene Ideen in Gruppen zu kommunizieren und nach Möglichkeit durchzusetzen. Die Studierenden erlangen die Kompetenz sich mit anderen Personen abzustimmen und durch die Kommunikation Synergieeffekte zu generieren.

Inhalt:
Die Studierenden sollen entsprechend ihrer zukünftigen Ausrichtung an Aufgaben mitarbeiten und Teilaufgaben selbstverantwortlich ausführen, deren Schwierigkeitsgrad dem Ausbildungsstand und den späteren Anforderungen in der betrieblichen Praxis angemessen ist.

prS: Praxisseminar

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Praxisseminar
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	150 Stunden, davon: 48 Stunden Präsenzzeit, 102 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	5
Semesterwochenstunden:	4
Veranstaltungstyp:	4 SWS Vorlesung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Seminar

Qualifikationsziele:

Fachkompetenz
- Kenntnis und Verstehen wichtiger Ansätze / Methoden / Modelle zur Verbesserung der interpersonalen Kommunikation

Methodenkompetenz
- Erkennen der Bedeutung der dargelegten Ansätze und Modelle für die berufliche Kommunikation
- Befähigung zur Einbringung des erlangten Wissens in das eigene Kommunikationsverhalten

Sozialkompetenz
- Verbesserung der eigenen Kommunikation und Metakommunikation
- Erlangung von Effektivität, Effizienz und Humanität im eigenen Kommunikationsverhalten
- Verbessertes Erkennen des eigenen / fremden Kommunikationsverhaltens
- Erlangung höheren Bewußtseins über das eigene / fremdes Kommunikationsverhalten

Inhalt:
- Hamburger Verständlichkeitskonzept
- Verhandlungsführung nach dem Hardvard-Konzept
- Transaktionsanalyse nach Eric Berne
- Menschliche Verhaltenssteuerung
- Kommunikationspsychologie nach Friedmann Schulz von Thun

Literatur

- Langer, Inghard; Schulz von Thun, Friedemann; Tausch, Reinhard: Sich verständlich ausdrücken. 10. völlig neubearbeitete Auflage. München: Ernst Reinhardt Verlag, 2015.
- Fisher, Roger; Ury, William; Patton, Bruce: Das Harvard-Konzept. Sachgerecht verhandeln – erfolgreich verhandeln. 20. Auflage. Frankfurt; New York: Campus Verlag GmbH, 2001
- Berne, Eric: Spiele der Erwachsenen. Psychologie der menschlichen Beziehungen. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag GmbH, 1991.
- Stewart, Ian; Joines, Vann: Die Transaktionsanalyse. Eine Einführung. 12. Auflage. Freiburg: Verlag Herder Freiburg im Breisgau, 2000.
- Häusel, Hans-Georg: Think Limbic! Die Macht des Unbewussten für Management und Verkauf. Freiburg: Haufe-Lexware GmbH & Co. KG, 2014.
- Schulz von Thun, Friedemann: Miteinander reden 1. Störungen und Klärungen. Allgemeine Psychologie der Kommunikation. Hamburg: Rowohlt Taschenbuch Verlag GmbH, Sonderausgabe April 2011.
- Schulz von Thun, Friedemann: Miteinander reden 3. Das "Innere Team" und situationsgerechte Kommunikation. Hamburg: Rowohlt Taschenbuch Verlag GmbH, Sonderausgabe April 2011.

prS: Praxisbegleitende Lehrveranstaltung

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Praxisbegleitende Lehrveranstaltung
Modulverantwortliche(r):	N.N.
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	90 Stunden, davon: 24 Stunden Präsenzzeit, 66 Stunden Vor- und Nachbereitung und Einübung des Lehrstoffs und Prüfungsvorbereitung
ECTS-Punkte:	3
Semesterwochenstunden:	2
Veranstaltungstyp:	2 SWS Vorlesung
Semesterturnus:	Sommersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Teilnahme und Studienarbeit oder Referat

Qualifikationsziele:

Fach- und Methodenkompetenz
Die Studierenden kennen die fachlichen Anforderungen an wissenschaftliche Abschlussarbeiten und mögliche Strategien, um diese zu erfüllen. Die Studierenden haben im Rahmen eines Arbeitsmusters bereits erste Erfahrungen mit wissenschaftlichem Arbeiten gemacht und kennen die typische Struktur einer wissenschaftlichen Abschlussarbeit.

Handlungskompetenz
Die Studierenden sind in der Lage eine erste wissenschaftliche Arbeit erfolgreich zu erstellen. Die Studierenden können selbständig korrekt zitieren und zielorientiert recherchieren.

Sozialkompetenz
Die Studierenden können ihren KommilitonInnen ihre wissenschaftliche Fragestellung schildern und im Team Lösungsstrategien entwickeln.

Inhalt: Die Lehrveranstaltung dient zur Vorbereitung auf die Bearbeitung des Bachelor-Projekts und der Bachelorarbeit. Grundlegende Methoden und Verfahren des wissenschaftlichen Arbeitens werden erläutert und anhand eines Arbeitsmusters eingeübt.
Literatur: ● Heesen, Wissenschaftliche Arbeiten schreiben mit Word 2016, Prescient, 2016

prS: Bachelorprojekt

Studiengang:	Bachelor Datenschutz und IT-Sicherheit
Modul:	Bachelorprojekt
Modulverantwortliche(r):	N.N./ ProfessorInnen des Bachelorstudienganges Datenschutz und IT-Sicherheit
Vorkenntnisse:	Schulwissen
Arbeitsaufwand:	120 Stunden, davon: 24 Stunden Präsenzzeit, 96 Stunden selbständiges Arbeiten am Projekt und Erstellung der Projektdokumentation
ECTS-Punkte:	4
Semesterwochenstunden:	2
Veranstaltungstyp:	Seminar
Semesterturnus:	Sommer- und Wintersemester
Unterrichtssprache:	Deutsch
Leistungsnachweis:	Projektarbeit und Dokumentation

Qualifikationsziele:

Handlungskompetenz
Die Studierenden erwerben die Kompetenz ein Projekt zur Vorbereitung ihrer Bachelorarbeit eigenständig und zielgerichtet zu definieren und ganz oder teilweise umzusetzen. Dabei erwerben sie die Fähigkeit Projekte zu dokumentieren und zu präsentieren.

Sozialkompetenz
Die Teilnehmer erwerben die Kompetenz vor einem kleineren Auditorium ein Projekt zu präsentieren und zu verteidigen. Dabei erlangen sie die Fähigkeit der Gruppe zu kommunizieren und zu diskutieren.

Inhalt:

- Planung und Umsetzung von individuellen Projekten aus dem Bereich des Datenschutzes und der IT-Sicherheit.
- Gestaltung von Präsentationen mit entsprechenden Visulisierungsprogrammen.
- Präsentationstechniken und Gestaltung von Vorträgen.
- Präsentation von Ergebnissen und oder Teilergebnissen aus laufenden Praxisprojekten.
- Darstellung aktueller Themen aus Projekten.