Digital Business University of Applied Sciences

Cybersecurity & Privacy (M.Sc.)

Modulhandbuch

Version: 09.2021

Abkürzungsverzeichnis

Abkürzung	Begriff
BSI	Bundesamt für Sicherheit in der Informationstechnik
CASB	Cloud Access Security Broker
CMDB	Configuration Management Database
DHL	Definite Hardware Library
ESA	Enterprise Security Arcitecture
FDA	Food and Drug Administration
ITIL	IT INfrastructure Library
LDA	Linear discriminant analysis
NLP	Natural Language Processing
OLA	Operational Level Agreement
PAM	Privileged Access Management
PCA	Principal component analysis
SABSA	Sherwood Applied Business Security Architecture
SAFe	Scaled Agile Framework
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOC	Security Operations Center
TAP	Test Access Port
TI	Threat Intelligence
TOGAF	The Open Group Architecture Framework

I. Vorwort

Der Master-Studiengang Cybersecurity & Privacy (Master of Science) umfasst vier Studiensemester in Vollzeit mit insgesamt 120 ECTS-Kreditpunkten. Dieser Studiengang kann nach individueller Vereinbarung auch in Teilzeit erfolgen. Die Regelstudiendauer verlängert sich dabei nach Maßgabe der Studien- und Prüfungsordnung für den Studiengang.

Forschung, wissenschaftlich fundierte Theorien und deren Transfer für die Berufspraxis sind handlungsleitend für das semi-virtuelle Lehr- und Lernkonzept.

Alle Module sind auf sechs CreditPoints (ECTS) zugeschnitten, da so

- eine zu isolierte Vermittlung von Lehrinhalten, die in einem engeren Bezug zueinander zu sehen und zu verstehen sind, vermieden wird,
- die Anzahl der Module für die Studierenden auf fünf je Semester begrenzt bleibt,
- den Studierenden die inhaltlichen Zusammenhänge und Wechselwirkungen bewusster werden,
- für die Studierenden die Prüfungsbelastungen (Anzahl der Prüfungen) zumutbar sind,
- den Lehrenden ein einheitlicherer, größerer Verantwortungsumfang für ein Modul anvertraut wird,
- die Anzahl der Lehrbeauftragten begrenzt werden kann und für diese das Engagement attraktiv bleibt.

Das Anspruchsniveau entspricht in allen Kursen internationalen Standards. Die Zugangsvoraussetzungen zum Studium sind in der Zulassungsordnung sowie in der Studien- und Prüfungsordnung der Digital Business University of Applied Sciences in der jeweils gültigen Fassung festgelegt.

II. Berufsprofil

Die digitale Transformation von Wirtschaft und Gesellschaft erfordert von Unternehmen enorme Anpassungen. Diese bergen Chancen, bringen aber auch neue Risiken mit sich. Die sichere digitale Transformation ist daher oberstes Gebot. Es bedarf eines qualifizierten Nachwuchses, der Unternehmen dabei unterstützt, ihre Chancen und Risiken auszubalancieren und insbesondere den Bereich der Cybersecurity umfassend zu betrachten.

Der Master-Studiengang Cybersecurity & Privacy hat sich die Ausbildung von Expert*innen zum Ziel gesetzt, die leitende, beratende oder selbständige Tätigkeiten im Bereich der Cybersecurity übernehmen.

Nach dem Studium bieten sich den Absolvent*innen mit dem in diesem Master-Studiengang erworbenen Kompetenzen zahlreiche Möglichkeiten für einen Karriereeinstieg oder -aufstieg in die Cybersecurity-Bereiche.

Absolvent*innen des Masterstudiengangs Cybersecurity & Privacy (M.Sc.) sind unter anderem in folgenden Positionen tätig:

- Chief Information Security Officer (CISO)
- Enterprise Security Architect
- Leiter*in der Informationssicherheit
- Unternehmensberater*in mit Schwerpunkt Cybersecurity
- Produktmanager*in für IT-Sicherheitslösungen
- Gutachter*in für Cybersecurity
- Zertifizierer*in für Cybersecurity
- Mitarbeiter*in / Leiter*in von Cyber Security Projekten
- Mitarbeiter*in / Leiter*in in Cyber/Informationssicherheits-Abteilungen zur Umsetzung von Cyber-Strategien

III. Studienziel

Der Cybersecurity kommt eine wesentliche Rolle bei Digitalisierungsvorhaben zu. Die Frequenz von Cyber- Angriffen, deren Intensität und Art verändern sich mit zunehmender Geschwindigkeit. Aber auch die Regulierung für Cybersicherheit und Anforderungen von Kund*innen, Lieferant*innen und Geschäftspartner*innen generell intensivieren sich. Um den vielfältigen Anforderungen von Organisationen gerecht werden zu können, fordern diese zunehmend Spezialist*innen auf dem Gebiet der Cybersecurity.

Reine Informatikfachkenntnisse reichen hier nicht mehr aus. Vielmehr ist dediziertes Cyber-Spezial- und Querschnittswissen notwendig, um den sicheren digitalen Wandel in Unternehmen konstruktiv zu begleiten. Genau dieser Aspekt wird im Master-Studiengang Cybersecurity & Privacy aufgegriffen, der neben der organisatorischen und juristischen Betrachtung von Cybersecurity auch die die technische Ausgestaltung von Systemen und Organisationen bis hin zum Management und zur Steuerung von Cybersecurity verbindet.

Der Studiengang bereitet somit ideal auf eine verantwortungsvolle Übernahme künftiger Aufgaben in der Cybersecurity vor.

Der Master-Studiengang Cybersecurity & Privacy vermittelt eine umfassende Ausbildung mit hohem Praxisbezug. Neben Pflichtmodulen haben die Studierenden die Möglichkeit, durch Wahlmodule eigene Schwerpunkte in den folgenden Bereich zu setzen:

- Managementsysteme für Sicherheit
- Kryptografie
- Technische Maßnahmen der Sicherheit

Der Studiengang vermittelt neben Methoden-, Prozess- und Technologiekompetenz auch Kompetenzen im Bereich Digital Leadership und wissenschaftliches Arbeiten. Studierende absolvieren damit nicht nur eine breite fachliche Ausbildung, sondern entwickeln auch Fähigkeiten zur kritischen Reflexion und wissenschaftlichen Analyse zentraler Herausforderungen der sicheren digitalen Transformation.

Studierende sind nach dem Abschluss des Masterstudiengangs u.a. befähigt, mittels geeigneter Methoden und Instrumente strategische Entscheidungen in der Cybersecurity zu treffen, sichere (digitale) Geschäftsmodelle und -Architekturen zu entwickeln und zu beurteilen und Transformationsprojekte im Kontext der Cybersecurity zu begleiten und umzusetzen.

Im anwendungsorientierten Studiengang Cybersecurity & Privacy (M.Sc.) wird die Vermittlung von Fach- und Methodenkompetenzen im Bereich Cybersecurity ergänzt um die Vermittlung spezifischer Fach- und Methodenkompetenzen im Bereich Prozess- und Technologiemanagement sowie managementspezifischer Kompetenzen wie Projektmanagement und Mitarbeiterführung. Außerdem erwerben die Studierenden ein breites Spektrum an Selbst- und Sozialkompetenzen.
Die Absolventinnen und Absolventen des Studiengangs können u.a.

- geeignete Methoden und Instrumente für strategische Entscheidungen in der Cybersecurity beurteilen, auswählen und anwenden;
- sichere (digitale) Geschäftsmodelle und -Architekturen entwickeln und beurteilen;
- Transformationsprojekte im Kontext der Cybersecurity begleiten und umsetzen;

- ethische und juristische Aspekte der Cybersicherheit identifizieren, geeignete Lösungskonzepte und -strategien auswählen und umsetzen;
- wissenschaftliche Erkenntnisse und Verfahren aus dem Bereich Cybersecurity & Privacy selbstständig anwenden und (weiter-)entwickeln;
- zentrale Herausforderungen der sicheren digitalen Transformation wissenschaftlich analysieren und kritisch reflektieren;
- komplexe und interdisziplinär angelegte Projekte unter Anwendung klassischer, hybrider und agiler Methoden erfolgsorientiert planen, organisieren und durchführen;
- (virtuelle) interdisziplinäre Teams verantwortungsvoll und effektiv führen sowie zielorientiert mit Personen aus verschiedenen Fachrichtungen, auch über digitale Medien, erfolgreich kommunizieren.

Der Master-Studiengang eignet sich für Absolvent*innen mit einem ersten berufsqualifizierenden Hochschulabschluss (Bachelorabschluss), vorzugsweise eines Informatik- sowie eines betriebswirtschaftlich orientierten Studiums. Der Studiengang richtet sich an Berufstätige unterschiedlichster Branchen- und Berufshintergründe, die ihr Wissen im Bereich Cybersecurity aufbauen und erweitern möchten.

IV. Übersicht über Module und Leistungsnachweise

Lfd. NR	Modul	Art der Lehrveran-staltung	Zugangs-voraus-setzung	Art der Prüfungs-leistung	ECTS-Kredit-punkte
(PLAN-)SEMESTER 1					
01	Einführung in die Grundlagen der Informationssicherheit	SK	Keine	KL	6
02	Rechtliche und ethische Aspekte der Cybersicherheit	SK	Keine	SL	6
03	Advanced Research Methods	SK	Keine	SL/ST	6
04	Grundlagen der IT für Cybersicher-heit	SK	Keine	SL	6
05	Grundlagen des IT Managements	SK	Keine	SL	6
(PLAN-)SEMESTER 2					
06	Einführung in die Grundlagen von Audits, Reviews und Assessments	SK	Keine	SL	6
07	Enterprise Security Architecture	SK	Keine	SL	6
08	Schwerpunktmodul 1	s.u.	s.u.	s.u.	6
09	Agiles Projektmanagement	SK	Keine	SL/ST	6
10	Data & Analytics	SK	Keine	SL	6
(PLAN-)SEMESTER 3					
11	Cloud Computing & Cloud Security	SK	Keine	SL	6
12	Schwerpunktmodul 2	s.u.	s.u.	s.u.	6
13	LoD & IS Lifecycle Management	SK	Keine	SL/ST	6
14	Schwerpunktmodul 3 - Forschungs-projekt	s.u.	s.u.	s.u.	6
15	Wahlpflichtmodul	s.u.	s.u.	s.u.	6
(PLAN-)SEMESTER 4					
16	Kolloquium & Schreibwerkstatt	L	Keine	SL	6
17	Masterarbeit	M	Anmel-dung MA	MA	24
Gesamt					**120**

Art der Lehrveranstaltung:

M Masterarbeitsprojekt

L Lab (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativen Lernen)

PR Projekt (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf problemorientiertem Lernen anhand eines konkreten realen oder fiktiven Projektauftrages)

SK Semi-virtueller Kurs (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen)

Art der Leistung:

MA Masterarbeit

K(xx) Klausur mit Dauer in Minuten

SL Studienbegleitende Leistungsnachweise
ST Studienarbeit/Projektarbeit/Dokumentation in Verbindung mit Referat/Präsentation

SCHWERPUNKTE
wählbare Schwerpunkte und Module im Studiengang Cybersecurity & Privacy (M.Sc.)
vgl. Anlage 2 Studien- und Prüfungsordnung

Lfd. NR	Modul	Art der Lehrver-anstal-tung	Zugangs-voraus-setzung	Art der Prüfungs-leistung	ECTS-Kredit-punkte
SCHWERPUNKT I: Managementsysteme für Sicherheit					
SPI-1	Einführung Managementsysteme und InfoSec-Standards	SK	Keine	SL/ST	6
SPI-2	Implementierung von Manage-mentsystemen	SK	Keine	SL	6
SPI-3	Forschungsprojekt	PR	Keine	SL	6
SCHWERPUNKT II: Technische Maßnahmen der Sicherheit					
SPII-1	Einführung in die technische Si-cherheit	SK	Modul 4	SL/ST	6
SPII-2	Entwicklung und Betrieb techni-scher Maßnahmen	SK	Modul 4	SL/ST	6
SPII-3	Forschungsprojekt	PR	Keine	SL	6
SCHWERPUNKT III: Kryptografie					
SPIII-1	Einführung in die Kryptografie	SK	Keine	K(120)	6
SPIII-2	Angewandte Kryptografie	L	Keine	SL/ST	6
SPIII-3	Forschungsprojekt	PR	Keine	ST	6

Art der Lehrveranstaltung:
M Masterarbeitsprojekt
L Lab (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativen Lernen)
PR Projekt (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf problemorientiertem Lernen anhand eines konkreten realen oder fiktiven Projektauftrages)
SK Semi-virtueller Kurs (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen)

Art der Leistung:
MA Masterarbeit
K(xx) Klausur mit Dauer in Minuten
SL Studienbegleitende Leistungsnachweise
ST Studienarbeit/Projektarbeit/Dokumentation in Verbindung mit Referat/Präsentation

WAHLPFLICHTMODULE
mögliche Wahlpflichtmodule im Studiengang Cybersecurity & Privacy (M.Sc.)
vgl. Anlage 3 Studien- und Prüfungsordnung

Lfd. NR	Modul	Art der Lehr-veran-staltung	Zugangs-voraus-setzung	Art der Prüfungs-leistung	ECTS-Kredit-punkte
WP1	Einführung Künstliche Intelligenz	SK	Keine	SL	6
WP2	Cybersecurity in Operational Tech-nology	SK	Keine	SL/ST	6
WP3	Cyber Resilience	SK	Keine	SL/ST	6
WP4	Design Thinking Methods: Product Development & Service Design	L	Keine	SL/ST	6

Art der Lehrveranstaltung:
M Masterarbeitsprojekt
L Lab (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativen Lernen)
PR Projekt (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf problemorientiertem Lernen anhand eines konkreten realen oder fiktiven Projektauftrages)
SK Semi-virtueller Kurs (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen)

Art der Leistung:
MA Masterarbeit
K(xx) Klausur mit Dauer in Minuten
SL Studienbegleitende Leistungsnachweise
ST Studienarbeit/Projektarbeit/Dokumentation in Verbindung mit Referat/Präsentation

V. Modulbeschreibungen

Die Studieninhalte sind übersichtlich in Module gebündelt; diese sind in ihrer Größe einheitlich (6 CP/ECTS) und auf Mindestgröße gebracht (vgl. European Communities: ECTS User´s Guide, Brussels 2015). Gemäß Musterrechtsverordnung §7 (Beschluss der Kultusministerkonferenz vom 07.12.2017) beinhalten die Modulbeschreibungen folgende Angaben

Credit Points/Workload	Benennung des Gesamtarbeitsaufwands und der Anzahl der zu erwerbenden Leistungspunkte für jedes Modul; Jedem Modul ist in Abhängigkeit vom Arbeitsaufwand für die Studierenden eine bestimmte Anzahl von ECTS-Leistungspunkten zuzuordnen.
Zeitrahmen	Mit dem Zeitrahmen ist festgelegt, in welchem Semester das Modul in den Studiengang eingeplant ist.
Dauer des Moduls	1 Semester
Häufigkeit	Festlegung, ob das Modul jedes Semester, jedes Studienjahr oder nur in größeren Abständen angeboten wird;

Qualifikationsziele: Lern- und Qualifikationsziele, die sich an der definierten Gesamtqualifikation (angestrebter Abschluss) ausrichten; Qualifikationsziele beschreiben das Wissen, die Fähigkeiten und Fertigkeiten der Studierenden, die sie zum berufsbezogenen Handeln befähigen.

Inhalte: Fachliche, methodische, fachpraktische und fächerübergreifende Inhalte dem betreffenden Modul bearbeitet werden.

Voraussetzungen für die Teilnahme: Unter den Voraussetzungen für die Teilnahme sind die Kenntnisse, Fähigkeiten und Fertigkeiten für eine erfolgreiche Teilnahme und Hinweise für die geeignete Vorbereitung durch die Studierenden zu benennen.

Verwendbarkeit: Es wird dargestellt, welcher Zusammenhang mit anderen Modulen desselben Studiengangs besteht und inwieweit es zum Einsatz in anderen Studiengängen geeignet ist.

Lehr- und Lernformen: Die Umsetzung des semi-virtuellen Studienkonzeptes in Bezug auf das Modul wird beschrieben.

Basisliteratur: Die Basisliteratur ist als Einstiegsempfehlung genannt und wird regelmäßig aktualisiert.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten: Prüfungsart, -dauer, -umfang werden beschrieben; sie können auf Antrag der bzw. des Lehrenden an den Prüfungsausschuss mit dessen Zustimmung geändert werden.

01 Einführung in die Grundlagen der Informationssicherheit

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die Grundlagen der Informationssicherheit und deren Einführung.
- Sie haben ein grundsätzliches Verständnis davon, was zur Einführung von Informationssicherheit auf Basis des internationalen Standards für Informationssicherheitsmanagementsysteme, ISO/IEC 27001, notwendig ist.
- Sie können auftretende Herausforderungen bei der Einführung von Informationssicherheit erkennen.

Inhalte

- Überblick zu den normativen Elementen des ISO/IEC 27001
- Der Managementsystemzyklus auf Basis des P-D-C-A
- Diskussion und Abgrenzung des Begriffs “Asset” aus Sicht der Informationsverarbeitung / Informationssicherheit
- Informationssicherheit, Sicherheitsziele und -strategien, Informationssicherheitsmanagementprozess
- Abgrenzung IT-Sicherheit vs. Informationssicherheit
- Gegenüberstellung der Standards ISO/IEC 27001 auf Basis von IT-Grundschutz (BSI, Bonn) vs. ISO/IEC 27001
- Stand und Entwicklung der Normenfamilie ISO/IEC 270XX (XX= 1,2,3,4,5..)
- Abgrenzung: Informationsmanagementsystem (IMS), Informationssicherheitsmanagementsystem (ISMS), IT Service Management (ITSM)
- Analysen von Schwachstellen und Bedrohungen in Abhängigkeit von Assets

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden

- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Kersten, H., Klett, G., Reuter, J. & Schröder, K. W. (2019). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Publishing.
- Humphreys, E. & Plate, A. (2013). *Are You Ready for an ISMS Audit Based on 27001?* BSI British Standards Institution.
- Benner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H. & Schaaf, T. (2019). *Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm DIN ISO/IEC 27001:2017*. Carl Hanser Verlag.
- Sowa, A. (2017). *Management Der Informationssicherheit: Kontrolle Und Optimierung*. Springer Vieweg.
- Schneier, B. (2009). *Schneier on Security*. Wiley.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Klausur (120 Minuten) (100%)

02 Rechtliche und ethische Aspekte der Cybersicherheit

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen ausgewählte Gesetze, die maßgeblich das Arbeitsumfeld der Cybersicherheit prägen.
- Die Studierenden können selbständig Arbeitskonflikte in der Cybersicherheit erkennen und thematisch zuordnen.
- Die Studierenden sind in der Lage, grundlegende ethische Aspekte der Cybersicherheit zu identifizieren und zu diskutieren.

Inhalte

- Datenschutzgrundverordnung
- §202 StGB (“Hackerparagraf”)
- Telekommunikationsgesetze
- Sozialgesetzbuch
- IT Sicherheitsgesetz / BSI Gesetz
- SEC Disclosure Guidance No 7
- Ethische Aspekte der Cybersicherheit (z.B. Überwachung versus Datenfreiheit)
- FDA und andere internationale Regularien

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Christen, M., Gordijn, B. & Loi, M. (2020). *The Ethics of Cybersecurity (The International Library of Ethics, Law and Technology (21))* (1st ed. 2020 Aufl.). Springer.

- Vedder, A., Schroers, J., Ducuing, C. & Valcke, P. (2019). *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security (7) (KU Leuven Centre for IT & IP Law Series)* (First Aufl.). Intersentia.
- Schneier, B. (2009). *Schneier on Security*. Wiley.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

03 Advanced Research Methods

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden haben ein fundiertes Verständnis von gängigen und fortgeschrittenen Methoden der empirischen Sozialforschung. Sie können qualitative und quantitativer Methoden entsprechend der wissenschaftlichen Fragestellung auswählen.
- Sie können geeignete Methoden der empirischen Sozialforschung, der Befragung, Beobachtung, quantitativ und qualitativer Methoden im Feld und im Labor, sowie der experimentellen Methoden auswählen und anwenden.

Inhalte

- Relevanz und Güte wissenschaftlicher Methoden
- Qualitative versus quantitative Methoden der Sozial- und Wirtschaftsforschung
- Erstellung von Studiendesigns, Skalenbildung, Methoden der Stichprobenauswahl
- Qualitative Forschungsmethoden (Tiefen- und Experteninterviews, Gruppendiskussionen, Ethnografische Beobachtungsstudien)
- Qualitative Analysemethoden (Inhaltsanalyse nach Mayring)
- Quantitative Forschungsmethoden (Befragungen, Beobachtungen, Experiment)
- Univariate und multivariate Analysemethoden (Regressionsanalyse, Einfaktorielle und multifaktorielle Varianzanalyse, Cluster- und Faktorenanalyse)
- Kritische Reflexion von Studienergebnissen und Integration in den bestehenden wissenschaftlichen Diskurs

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Data Science & Management (M.Sc.)
- Digital Responsible Leadership (M.Sc.)
- Cyber Security & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden

- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Backhaus, K. Erichson, B., Plinke, W. & Weiber, R. (1994). *Multivariate Analysemethoden. Eine anwendungsorientierte Einführung* (11. überarbeitete Auflage). Berlin: Springer.
- Baur, N. & Blasius, J. (2019). *Handbuch Methoden der empirischen Sozialforschung.* Wiesbaden: Springer Vieweg.
- Fahrmeir, L., Heumann, C., Künstler, R., Pigeot, I. & Tutz, G. (2016). *Statistik.* Springer Berlin Heidelberg.
- Mayring, P. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12. Auflage). Weinheim: Julius Beltz.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)

- studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)

04 Grundlagen der IT für Cybersicherheit

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen typische IT Komponenten für Cybersicherheit.
- Sie sind in der Lage, IT Komponenten und ihre Bedeutung in den Bereichen Prävention, Detektion, Abwehr und Forensik zu verstehen.
- Sie verstehen grundsätzlich, wie IT Systeme für Cybersicherheit innerhalb der "Cybersecurity Kill Chain" verwendet werden können.
- Sie sind in der Lage, die Interaktionen von IT für Cybersecurity zu verstehen, anzuwenden und zu bewerten
- Sie sind in der Lage, diese IT Systeme in einer Enterprise Security Architecture anzuwenden.

Inhalte

- Threat Intelligence
- Threat Detection
- PAM Software
- Secure Logging
- Time Synchronization
- Next Gen Firewall
- Endpoint Protection
- Ticket Systems
- SOC Design
- Network TAPping

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden

- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Eckert, C. (2018). *IT-Sicherheit*. De Gruyter.
- Muniz, J., Frost, M. & Santos, O. (2020). *The Modern Security Operations Center*. Pearson Education (US).
- Thomas, A. E. (2018). *Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence*. CreateSpace Independent Publishing Platform.
- Department of the Army. (2019). *Reconnaissance and Security Operations*. Independently published.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

05 Grundlagen des IT Managements

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden erlangen einen grundlegenden Einblick in das IT Management als Grundlage für den IT Betrieb. Sie verstehen die sich daraus ableitenden Anforderungen an die Cybersicherheit.
- Die Studierenden sind in der Lage, die IT Infrastructure Library (ITIL) als Grundlage von allgemeinen Management- und Service-Management-Praktiken anzuwenden.
- Sie können eigenständig einfache IT Management Aufgaben identifizieren, klassifizieren und Lösungen ableiten.

Inhalte

- Aufbau von ITIL
- Allgemeine Management-Praktiken
- Service-Management-Praktiken
- SLA und OLA Definition
- Problem Management und Incident Management
- CMDB und DHL
- IT Accounting und Auswirkung auf Transfer Pricing
-

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Urbach, N. & Ahlemann, F. (2016). *IT-Management im Zeitalter der Digitalisierung*. Springer Publishing.

- Hoch, D. J., Klimmer, M. & Leukert, P. (2005). *Erfolgreiches IT-Management im öffentlichen Sektor: Managen statt verwalten*. Gabler Verlag.
- Tiemeyer, E. (2020). *Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis*. Carl Hanser Verlag.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

06 Einführung in die Grundlagen von Audits, Reviews und Assessments

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die grundlegenden Auditprinzipien sowie die ethischen und fachlichen Anforderungen an Auditor*innen.
- Sie können zwischen den verschiedenen Auditarten und Reviews unterscheiden und wissen, wann welche Auditart von Relevanz ist.
- Sie können sowohl interne wie externe Audit Programme planen, erstellen und koordinieren.
- Sie sind in der Lage, selbständig Audits durchzuführen.
- Sie kennen die Dokumentationsanforderungen im Rahmen von Audits sowohl aus Sicht von Auditierenden als auch aus Sicht von Auditierten.
- Sie sind in der Lage, einen Auditbericht zu strukturieren und zu verfassen.
- Sie sind mit der Fragetechnik im Rahmen von Audits vertraut und können diese bewusst und selbständig anwenden.

Inhalte

- Begriffsbestimmungen und Abgrenzungen im Kontext Audit, Review und Assessment
- Auditmethoden
- Umgang mit Feststellungen/Abweichungen
- Leiten und Lenken eines Auditprogramms
- Auditdurchführung
- Abschließen des Audits
- Durchführung von Auditfolgemaßnahmen
- Kompetenzen von und Bewertungen durch Auditor*innen

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden

- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- DIN EN ISO 17021:-1:2015-11
- DIN EN ISO 19011:2018-10
- DIN EN ISO/IEC 27000:2020-06
- Kersten, H., Klett, G., Reuter, J. & Schröder, K. W. (2019). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Publishing.
- Humphreys, E. & Plate, A. (2013). *Are You Ready for an ISMS Audit Based on 27001?* BSI British Standards Institution.
- Benner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H. & Schaaf, T. (2019). *Praxis-buch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm DIN ISO/IEC 27001:2017*. Carl Hanser Verlag.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

07 Enterprise Security Architecture (ESA)

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden können Enterprise (Security) Architecture Management auf die Zusammenhänge von Software- und Organisationsentwicklung anwenden.
- Die Studierenden können IT Sicherheits-Systemlösungen entwickeln und auf sich verändernde Geschäftsprozesse anwenden.
- Die Studierenden haben ein Verständnis dafür, wie technologische Fortschritte in Sicherheitsarchitekturen umgesetzt werden können.
- Sie können den Einfluss von Sicherheitsarchitekturen auf diverse Stakeholder, wie Mitarbeiter, Kunden und Lieferanten beurteilen.
- Die Studierenden sind in der Lage, die erworbenen Kenntnisse in Form von methodischen Ansätzen zur Weiterentwicklung von Organisationen und Architekturen einzusetzen.
- Die Studierenden sind in der Lage, Funktionen und die entsprechende Governance von ESA zu beschreiben und anzuwenden.
- Sie kennen verschiedene Rahmenwerke und sind in der Lage, für die jeweilige Aufgabenstellung das jeweils angemessene Rahmenwerk zu selektieren und anzuwenden.

Inhalte

- Grundlagen von Enterprise Security Architecture als integraler Bestandteil der Enterprise Architecture
- Grundlagen und Einsatz von ESA/ EA Frameworks: Vorstellung zentraler Grundideen von Rahmenwerken und Diskussion an Beispielen.
- IT-Anwendungsportfoliomanagement
- Architektur-Governance
- Modellierung von Unternehmenssicherheitsarchitekturen
- Querschnittsaufgaben und Zusammenhänge zur Unternehmensarchitektur
    - IT Service Management
    - IT Governance mit Hilfe von COBIT®

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Dern, G. (2009). *Management Von It Architekturen: Leitlinien für die Ausrichtung, Planung und Gestaltung von Informationssystemen* (3. Aufl.). Springer Vieweg.
- Weill, P. & Ross, J. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Review Press.
- Hanschke, I. (2010). *Strategisches Management der IT-Landschaft. Ein praktischer Leitfaden für das Enterprise Architecture Management.* (2. Aufl.). Carl Hanser Verlag.
- Keller, W. (2012. *IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung.* (2. Aufl.). (2012). dpunkt.verlag.
- Keuntje, J. H. & Barkow, R. (2010). *Enterprise-architecture-Management in der Praxis. Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen.* Symposion.
- Ross, J. W., Weill, P. & Robertson, D. (2006). *Enterprise Architecture As Strategy: Creating a Foundation for Business Execution*. Harvard Business Review Press.
- Schwarzer, B. (2009). *Einführung in das Enterprise Architecture Management. Verstehen - Planen - Umsetzen*. Books on Demand.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

08 Schwerpunktmodul 1

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Siehe Beschreibung der Schwerpunktmodule

09 Agiles Projektmanagement

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die Grundlagen und Begriffe des klassischen und des agilen Projektmanagements. Sie kennen zentrale agile Methoden und deren Vorgehensweise sowie korrespondierende agile Tools und Techniken.
- Sie sind in der Lage, klassische und agile Projektmanagementmethoden in der Praxis anzuwenden.
- Die Studierenden haben ein Grundverständnis von Agilität und damit zusammenhängenden Werten und Prinzipien. Sie verstehen, wie Agilität im Projektmanagement förderlich eingesetzt werden kann.
- Die Studierenden kennen die Rollen und Verantwortlichkeiten in der agilen Projektarbeit (insb. Scrum) und können diese aktiv in der Praxis anwenden. Sie sind in der Lage, Projekte erfolgreich zu leiten und entsprechende Arbeitspakete zu übernehmen.
- Die Studierenden kennen hybride Formen des Projektmanagements. Sie sind in der Lage, klassische Projektmanagement-Ansätze auch in komplexen Umwelten zu nutzen und sie mit agilen Techniken zu verknüpfen.
- Die Studierenden kennen agile Veranstaltungsformate. Sie sind dazu fähig, die Transformation einer Organisation zu mehr Agilität und Dynamik erfolgreich mitzugestalten.

Inhalte

- Grundlagen und klassisches Projektmanagement
- Agiles Projektmanagement
  - Agilität im Kontext des Projektmanagements, agile Werte und Prinzipien
  - Agile Methoden und Vorgehensweisen (z.B. Scrum, Kanban, Lean-Startup)
  - Rollenverständnisse und korrespondierende Verantwortungsbereiche in agilen Methoden (insb. Scrum)
  - Agile Tools und Arbeitstechniken (z.B. User Stories, Epics, Persona, Planungspoker, Story- und Valuepoint Schätzung, Timeboxing, Daily Standup, Taskboarding, Definition of Done, Burn Down Charts)
  - Agiles Controlling und Qualitätsmanagement
- Hybrides Projektmanagement
  - Begriffsklärung
  - Formen und Vorgehensweisen
- Agile Veranstaltungsformate (z.B. Google Design Sprint, Hackathon, FedEx days, Rotation Days, FedEx Meetings, Barcamp, ThinkTank)
- Umsetzung konkreter Projektaufgaben an Hand agiler und hybrider Ansätze

Voraussetzungen für die Teilnahme
keine

Verwendbarkeit
- Digital Business Management (M.Sc.)
- Data Science & Management (M. Sc.)
- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs
- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Adkins, L. (2010). *Coaching Agile Teams: A Companion for ScrumMasters, Agile Coaches, and Project Managers in Transition*. Addison-Wesley Professional.
- Graf, N., Gramß, D. & Edelkraut, F. (2019). *Agiles Lernen: Neue Rollen, Kompetenzen und Methoden im Unternehmenskontext* (2. Aufl.). Haufe.
- Kuster, J., Bachmann, C., Huber, E., Hubmann, M., Lippmann, R., Schneider, E., Schneider, P., Witschi, U. & Wüst, R. (2019). *Handbuch Projektmanagement: Agil – Klassisch – Hybrid* (4. Aufl.). Springer.
- Poguntke, S. (2014). *Corporate Think Tanks: Zukunftsgerichtete Denkfabriken, Innovation Labs, Kreativforen & Co.* Springer.
- Timinger, H. (2017). *Modernes Projektmanagement: Mit Traditionellem, Agilem Und Hybridem Vorgehen Zum Erfolg*. Wiley.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
- Studienbegleitende Leistungsnachweise (50%)
- Studienarbeit (50%)

10 Data & Analytics

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden können die Begriffe Big Data und Data Analytics definieren, einordnen und anwenden.
- Sie können eigenständig Datenstrukturen modellieren und sind dazu in der Lage, Daten verschiedenster Dimensionen mit Hilfe von Clustering und Supervised Learning zu analysieren.
- Die Studierenden können Methoden zur Text- und Dokumentenanalyse anwenden.
- Sie können mit komplexeren Informationen (z.B. Risikoanalysen, raumbezogene und temporale Daten) umgehen, diese analysieren und visualisieren.

Inhalte

- Definitionen und Konzepte von Big Data und Data Analytics
  - Datentypen, mehrdimensionale Daten, Dimensionsreduktion (PCA, LDA)
  - Predictive, Descriptive, Prescriptive Analytics
  - Qualitative vs quantitative Analysen
- Data Preparation
- Clustering
- Supervised Learning
- Text- und Dokumentenanalyse, Grundlagen des Natural Language Processing (NLP Pipeline)
- Geospatial Data Analytics und Temporal Data Analytics

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Ward, M. O., Grinstein, G. & Keim, D. (2015). *Interactive Data Visualization: Foundations, Techniques, and Applications*. A K Peters/CRC Press.
- Telea, A. C. (2007). *Data Visualization: Principles and Practice*. A K Peters/CRC Press.
- Haneke, U., Trahasch, S., Zimmer, M. & Felden, C. (2019). *Data Science: Grundlagen, Architekturen und Anwendungen*. Dpunkt.Verlag GmbH.
- Wickham, H. & Grolemund, G. (2017). *R for Data Science: Import, Tidy, Transform, Visualize, and Model Data*. O'Reilly Media.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

11 Cloud Computing & Cloud Security

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden sind in der Lage, unterschiedliche Cloud Service Modelle zu differenzieren (PaaS, SaaS, IaaS).
- Sie verstehen die Differenzierung zwischen Public Cloud, Private Cloud und Hybrid Cloud.
- Sie sind in der Lage, wesentliche Elemente der Cloud Security für vorliegende Liefer-Situationen selbständig zu erkennen, auf die jeweilige Liefersituation anzupassen und zu designen.
- Die Studierenden kennen wesentliche technische Komponenten der Cloud Security, wie z.B. CASBs, Klassifizierungstechnologien, Verschlüsselungstechnologien, Cloud-based Directory Services.
- Sie kennen wesentliche Standards in der Auditierung von Cloud Services (z.B. Star Audit, ISO/IEC 27018, …).

Inhalte

- Grundlagen und Begriffe zu Cloud Services
- Cloud Service Modelle:
  - IaaS
  - PaaS
  - SaaS
- Cloud Delivery Modelle:
  - Public
  - Hybrid
  - Private
- Cloud Security Komponenten
- Audit Standards für Cloud Computing
- Security Controls für Cloud Computing
- Cloud Access Security Broker
- Directory Technologien
- Verschlüsselungssoftware für die Cloud

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Krcmar, H., Leimeister, J. M., Roßnagel, A. & Sunyaev, A. (2016). *Cloud-Services aus der Geschäftsperspektive*. Springer Publishing.
- Jr., M. G. B. & Jackson, K. L. (2016). *Practical Cloud Security: A Cross-Industry View*. CRC Press.
- Dotson, C. (2019). *Practical Cloud Security: A Guide for Secure Design and Deployment*. O'Reilly Media.
- Information Resources Management Association. (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications*. IGI Global.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

Studienbegleitende Leistungsnachweise (100%)

12 Schwerpunktmodul 2

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Siehe Beschreibung der Schwerpunktmodule

13 LoD & IS Lifecycle Management

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die Details des Lines of Defense Modells (LoD).
- Sie sind in der Lage, die Rollen der Bereiche Governance, Operations und Compliance zu unterscheiden und anzuwenden.
- Sie sind in der Lage, Sicherheitsarchitekturen mit dem LoD-Modell zu mappen und können Maßnahmen der entsprechenden Line of Defense zuordnen.
- Die Studierenden sind in der Lage, in verschiedenen Industrien das LoD Modell anzuwenden.

Inhalte

- Aufbau des Line of Defense Modells
- Regulatorische und Compliance Anforderungen an das LoD-Modell
- Ableitung von Aufbau und Ablauforganisationen aus dem LoD-Modell
- Anwendung des LoD-Modells mit Blick auf COSO

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Falk, M. (2012). *IT-Compliance in der Corporate Governance: Anforderungen und Umsetzung*. Gabler Verlag.
- Santos, O. (2018). *Developing Cybersecurity Programs and Policies*. Pearson Education.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)

- Studienbegleitende Leistungsnachweise 40%
- Studienarbeit 60%

14 Schwerpunktmodul 3 - Forschungsprojekt

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Siehe Beschreibung der Schwerpunktmodule

15 Wahlpflichtmodul

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Siehe Beschreibung der Wahlpflichtmodule

16 Kolloquium & Schreibwerkstatt

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	4. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden können komplexe fachliche Herausforderungen und Lösungen wissenschaftlich sowohl schriftlich als auch mündlich argumentativ vertreten.
- Sie können theoretische und methodische Herangehensweisen zur Bearbeitung der wissenschaftlichen Fragestellung und Hypothesen darlegen und begründen.
- Sie sind in der Lage, die Folgen ihrer Entscheidungen fachlich einzuschätzen und ihre Handlungen und Entscheidungen kritisch zu reflektieren.
- Die Studierenden sind in der Lage, mit ihrem Thema der Masterarbeit verwandte Problem- und Fragestellungen zu erkennen und Lösungsmöglichkeiten aufzuzeigen.
- Die Studierenden sind in der Lage, ihren Arbeitsprozess und ihre Arbeitsergebnisse im Rahmen des Masterarbeitsprojektes zielgerichtet und zielgruppenspezifisch gegenüber fachlich nicht tief bewanderten Personen und Fachvertreter*innen darstellen und präsentieren.

Inhalte

- Fachliche Orientierung an den Themen der Abschlussarbeiten
- wissenschaftlicher Forschungsprozess
- Wissenschaftliche Literaturrecherche zum Themenschwerpunkt
- Argumentation und Interpretation von Studienergebnissen
- Zielgruppenspezifische Präsentation von Studienergebnissen mit digitalen Medien

Voraussetzungen für die Teilnahme

- Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Data Science & Management (M.Sc.)
- Digital Responsible Leadership (M.Sc.)
- Cyber Security & Privacy (M.Sc.)

Lehr- und Lernformen: Lab

virtuelle Lehrveranstaltungen mit optionalen Präsenzveranstaltungen mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativen Lernen

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Übungen auf der Online-Lernplattform (z.B. Quizzes, individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)

- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten
- Arbeit in (virtuellen) Forschungsteams

Basisliteratur
Themenspezifische Fachliteratur wird in der Lehrveranstaltung bekannt gegeben.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

17 Masterarbeit

Credit Points/Workload	24 CP (ECTS) / 600 Stunden Selbstlernzeit: 600 Stunden
Zeitrahmen	4. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden können das im Masterstudiengang erworbene Wissen für die Bearbeitung einer ausgewählten Problemstellung nutzen.
- Sie können eine wissenschaftliche Fragestellung aus dem gewählten Themenbereich selbstständig unter Berücksichtigung des aktuellen Forschungsstandes und unter Berücksichtigung der Regeln wissenschaftlichen Arbeitens innerhalb einer vorgeschriebenen Zeit bearbeiten.
- Die Studierenden sind dazu in der Lage zu beurteilen, welche methodologischen Zugänge bzw. wissenschaftlichen Forschungsmethoden für die Bearbeitung einer selbst gewählten Fragestellung geeignet sind. Sie können diese praxisbezogen anwenden.
- Sie können die gewonnenen Erkenntnisse beschreiben und bewerten, sie in den Forschungsstand einordnen und den Forschungsprozess kritisch reflektieren.
- Sie können den gewählten wissenschaftlichen Standpunkt sowie die verwendeten Methoden und gewonnenen Ergebnisse logisch ableiten, schriftlich darlegen und argumentativ verteidigen.
- Die Studierenden sind dazu in der Lage, einen Beitrag zum Theorie-Praxis-Transfer zu leisten und das während des Studiums erworbene disziplinäre Wissen in die berufliche Praxis zu integrieren.

Inhalte

- Eigenständige Bearbeitung einer wissenschaftlichen Problemstellung
- Kritische Reflexion des Forschungsstandes.

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Cybersecurity & Privacy (M.Sc.)
- Data Science & Management (M.Sc.)
- Digital Responsible Leadership (M.Sc.)

Lehr- und Lernformen:

- eigenständiges Verfassen einer Masterarbeit
- individuelle Begleitung bei Themenauswahl und methodischem Vorgehen durch Fachbetreuer*innen

Basisliteratur

- Themenspezifische Fachliteratur wird in der Lehrveranstaltung bekannt gegeben.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Masterarbeit (100%)

SCHWERPUNKT I: Managementsysteme für Sicherheit

SPI-1 Einführung Managementsysteme und InfoSec-Standards

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen verschiedene Managementsystem- und Sicherheitsstandards.
- Sie können, je nach Anwendungssituation, einen angemessenen Sicherheitsstandard auswählen und einsetzen.
- Die Studierenden sind in der Lage eigene Managemenstsysteme zu implementieren und zu betreiben.
- Sie können Synergieeffekte durch den Einsatz der unterschiedlichen Managementsystemen erkennen und nutzen.
- Die Studierenden sind in der Lage, Sicherheitsstandards in etablierten Managementsystemen zu verwenden.

Inhalte

- ISO/IEC 27000 Familie
- ISO/IEC 22301
- ISO/IEC 20000
- ISO/IEC 9000
- ISO/IEC 14000
- ISO/IEC 15000
- BSI Grundschutz auf Basis ISO/IEC 27001

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden

- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Kersten, H., Klett, G., Reuter, J. & Schröder, K. W. (2019). IT-Sicherheitsmanagement nach der neuen ISO 27001. Springer Publishing.
- Benner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H. & Schaaf, T. (2019). Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm DIN ISO/IEC 27001:2017. Carl Hanser Verlag.
- Sowa, A. (2017). Management Der Informationssicherheit: Kontrolle Und Optimierung. Springer Vieweg.
- Eckert, C. (2018). IT-Sicherheit. De Gruyter.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)

- Studienbegleitende Leistungsnachweise 40%
- Studienarbeit 60%

SPI-2 Implementierung von Managementsystemen

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen Good Practices, Risiken sowie die kritischen Erfolgsfaktoren für die Implementierung von Managementsystemen.
- Sie kennen die gängigen Schritte bei der Einführung von Managementsystemen und können einen konkreten Plan zur Implementierung eines Managementsystems entwerfen.
- Die Studierenden sind in der Lage, ein Managementsystem mit seinen Prozessen und Strukturen unter Berücksichtigung der jeweiligen Gegebenheiten und Anforderungen von Organisationen zu planen.
- Sie können eigenständig das Managementsystem mit seinen Prozessen und Strukturen in einer Organisation implementieren und betreiben.
- Sie sind befähigt, die Performance des Managementsystems zu messen, zu bewerten und kontinuierlich zu verbessern.

Inhalte

- Grundlagen der Implementierung von Managementsystemen anhand von Praxisbeispielen (Good Practices, Risiken und Fallstricke, kritische Erfolgsfaktoren, etc.)
- Projektplanung zur Implementierung eines Managementsystems am Beispiel eines ausgewählten Managementsystems wie z.B. Informationssicherheitsmanagementsystem (ISMS)
- Planung der Prozesse und Strukturen eines Managementsystems am Beispiel eines ausgewählten Managementsystems
- Implementierung und Betrieb von Prozessen und Strukturen eines Managementsystems am Beispiel eines ausgewählten Managementsystems
- Messung, Bewertung und Verbesserung der Performance eines Managementsystems am Beispiel eines ausgewählten Managementsystems

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform

- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- BSI Grundschutzkatalog (in der jeweils aktuellsten Version. Online)
- Kersten, H., Klett, G., Reuter, J. & Schröder, K. W. (2019). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Publishing.
- Benner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H. & Schaaf, T. (2019). *Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm DIN ISO/IEC 27001:2017*. Carl Hanser Verlag.
- Sowa, A. (2017). *Management Der Informationssicherheit: Kontrolle Und Optimierung*. Springer Vieweg.
- Clader, A. (2016). *Nine Steps to Success: An ISO 27001 Implementation Overview*. IT Governance Limited.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

SPI-3 Forschungsprojekt

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden sind in der Lage, wissenschaftliche Fragestellungen und Hypothesen zu formulieren.
- Sie können geeignete wissenschaftliche Publikationen auswählen und verstehen.
- Sie verstehen den Einsatz empirischer Methoden zur Erlangung wissenschaftlicher Erkenntnisse und können diese anwenden. Sie können Forschungsmethoden zur Beantwortung wissenschaftlicher Hypothesen kritisch reflektieren.
- Sind in der Lage, Ergebnisse von empirischen Forschungsprozessen korrekt zu interpretieren, darzustellen und kritisch zu reflektieren.
- Die Studierenden sind in der Lage, effektiv in remoten Arbeitsgruppen an einem gemeinsamen Projekt zu arbeiten.

Inhalte

- Entwicklung einer Forschungsfrage mit thematischem Bezug zum Schwerpunkt
- Durchführung einer Literaturrecherche und Aufbereitung des aktuellen Forschungsstandes zur Forschungsfrage
- Formulierung von Hypothesen auf Basis einer gewählten Bezugstheorie bzw. des aktuellen Forschungstandes
- Wahl und Durchführung einer geeigneten empirischen Methode zur Überprüfung der Hypothesen inkl. Operationalisierung der relevanten Konstrukte, Erhebung von Primärdaten oder Recherche von Sekundärdaten sowie Datenauswertung
- Interpretation und kritische Reflexion der Ergebnisse
- Ableitung wissenschaftlicher und praktischer Implikationen
- Dokumentation des gesamten Forschungsprojekts in einer Projektarbeit
- Vorbereitung und Durchführung einer wissenschaftlichen Präsentation der Ergebnisse

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Data Science & Management (M.Sc.)
- Cybersecurity & Privacy (M.Sc.)

- Digital Responsible Leadership (M.Sc.)

Lehr- und Lernformen: Projekt
virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf problemorientiertem Lernen anhand eines konkreten realen oder fiktiven Projektauftrages

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Übungen auf der Online-Lernplattform (z.B. Quizzes, individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten
- Projektarbeit in (virtuellen) Teams

Basisliteratur

- Backhaus, K. Erichson, B., Plinke, W. & Weiber, R. (1994). Multivariate Analysemethoden. Eine anwendungsorientierte Einführung (11. Überarbeitete Auflage). Berlin: Springer.
- Baur, N. & Blasius, J. (2019). Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer Vieweg.
- Brühl, R. (2017). Wie Wissenschaft Wissen schafft: Wissenschaftstheorie und-ethik für die Sozial-und Wirtschaftswissenschaften. UTB: Stuttgart
- Theisen, M. R. & Theisen, M. (2013). Wissenschaftliches Arbeiten: Erfolgreich bei Bachelor- und Masterarbeit; [das Standardwerk neu konzipiert (16., vollst. überarb. Aufl.). Vahlen: München.
- Wiltinger, K. & Wiltinger, A. (2014). Wissenschaftliches Arbeiten: Praxisleitfaden für Studierende. Cuvillier: Göttingen
- Wissenschaftliche Paper zur gewählten Forschungsfrage

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

SCHWERPUNKT II: Technische Maßnahmen der Sicherheit

SPII-1 Einführung in die technische Sicherheit

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden können eigenständig eine risikoorientierte Enterprise Security Architecture entwickeln und IT Systeme für Cybersicherheit einführen.
- Die Studierenden haben ein vertieftes Verständnis der Einsatzmöglichkeiten von Technologien im Rahmen der Prävention, Detektion und Abwehr. Sie können Einsatzchancen und Limitationen verstehen, erläutern und bewerten.
- Die Studierenden kennen verschiedene Technologien und Tools und können sie anwenden, um eigene Sicherheitsanalysen vorzunehmen.
- Die Studierenden kennen gängige Frameworks für Penetration Testing und können sie anwenden.

Inhalte

- Threat Detection
- SIEM
- Next Gen Firewalls
- Endpoint Protection
- Armitage Framework
- Kali Framework
- Shodan.IO
- Metasploit

Voraussetzungen für die Teilnahme

Modul 4: Grundlagen der IT für Cybersicherheit

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden

- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Messner, M. (2017). *Hacking mit Metasploit: Das umfassende Handbuch zu Penetration Testing und Metasploit*. Dpunkt.Verlag GmbH.
- Jaswal, N. (2017). *Metasploit Bootcamp: The fastest way to learn Metasploit*. Packt Publishing.
- Matherly, J. (2016). *Complete Guide to Shodan*. Leanpub. https://leanpub.com/shodan
- Ebner, J. (2020). *Einstieg in Kali Linux: Penetration Testing und Ethical Hacking mit Linux*. MITP Verlags GmbH.
- B, M. (2017). *Hacken mit Kali-Linux*. Books on Demand.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)

- Studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)

SPII-2 Entwicklung und Betrieb technischer Maßnahmen

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Studierende haben ein erweitertes Verständnis der IT Komponenten und Systeme für Cybersicherheit.
- Die Studierenden verstehen technologische Maßnahmen und können den kontinuierlichen Betrieb technologischer Lösungen für Cybersicherheit beschreiben.
- Die Studierenden kennen insbesondere typische technologische Komponenten eines Security Operation Centers und können sie betreiben.
- Sie kennen den Prozess zur Entwicklung von Playbooks für den SOC Betrieb und können eigene Playbooks entwickeln.
- Die Studierenden kennen die Anforderung an “Transition & Transformation (T&T)” bei der Einrichtung von Security Operations Centern und sind in der Lage, eigene “T&T” Projekte zu planen.

Inhalte

- Planung, Einsatz und Betrieb von Threat Detection Systemen
- Anwendung von SIEM Systemen, sowie die Gestaltung von Playbooks für SOC und SIEM
- Einsatz von Next Gen Firewalls und deren Limitationen, sowie die Nutzung von Analytik Möglichkeiten (z.B. Metadaten und Telemetrie-Informationen)
- Endpoint Protection Möglichkeiten inklusive der Möglichkeit der Auswertung für forensische Zwecke
- Integration von Endpoint Protection mit Perimeter Security & Next Gen Firewalls
- Transition & Transformation Projekte im Fokus der Integration von Daten- und Eventquellen mit Sicherheitstechnologien

Voraussetzungen für die Teilnahme

Modul 4: Grundlagen der IT für Cybersicherheit

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)

- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Messner, M. (2017). *Hacking mit Metasploit: Das umfassende Handbuch zu Penetration Testing und Metasploit*. Dpunkt.Verlag GmbH.
- Jaswal, N. (2017). *Metasploit Bootcamp: The fastest way to learn Metasploit*. Packt Publishing.
- Matherly, J. (2016). *Complete Guide to Shodan*. Leanpub. https://leanpub.com/shodan
- Ebner, J. (2020). *Einstieg in Kali Linux: Penetration Testing und Ethical Hacking mit Linux*. MITP Verlags GmbH.
- B, M. (2017). *Hacken mit Kali-Linux*. Books on Demand.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)

- Studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)

SPII-3 Forschungsprojekt

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden sind in der Lage, wissenschaftliche Fragestellungen und Hypothesen zu formulieren.
- Sie können geeignete wissenschaftliche Publikationen auswählen und verstehen.
- Sie verstehen den Einsatz empirischer Methoden zur Erlangung wissenschaftlicher Erkenntnisse und können diese anwenden. Sie können Forschungsmethoden zur Beantwortung wissenschaftlicher Hypothesen kritisch reflektieren.
- Sind in der Lage, Ergebnisse von empirischen Forschungsprozessen korrekt zu interpretieren, darzustellen und kritisch zu reflektieren.
- Die Studierenden sind in der Lage, effektiv in remoten Arbeitsgruppen an einem gemeinsamen Projekt zu arbeiten.

Inhalte

- Entwicklung einer Forschungsfrage mit thematischem Bezug zum Schwerpunkt
- Durchführung einer Literaturrecherche und Aufbereitung des aktuellen Forschungsstandes zur Forschungsfrage
- Formulierung von Hypothesen auf Basis einer gewählten Bezugstheorie bzw. des aktuellen Forschungstandes
- Wahl und Durchführung einer geeigneten empirischen Methode zur Überprüfung der Hypothesen inkl. Operationalisierung der relevanten Konstrukte, Erhebung von Primärdaten oder Recherche von Sekundärdaten sowie Datenauswertung
- Interpretation und kritische Reflexion der Ergebnisse
- Ableitung wissenschaftlicher und praktischer Implikationen
- Dokumentation des gesamten Forschungsprojekts in einer Projektarbeit
- Vorbereitung und Durchführung einer wissenschaftlichen Präsentation der Ergebnisse

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Data Science & Management (M.Sc.)
- Cybersecurity & Privacy (M.Sc.)
- Digital Responsible Leadership (M.Sc.)

Lehr- und Lernformen: Projekt
virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf problemorientiertem Lernen anhand eines konkreten realen oder fiktiven Projektauftrages

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Übungen auf der Online-Lernplattform (z.B. Quizzes, individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten
- Projektarbeit in (virtuellen) Teams

Basisliteratur

- Backhaus, K. Erichson, B., Plinke, W. & Weiber, R. (1994). Multivariate Analysemethoden. Eine anwendungsorientierte Einführung (11. Überarbeitete Auflage). Berlin: Springer.
- Baur, N. & Blasius, J. (2019). Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer Vieweg.
- Brühl, R. (2017). Wie Wissenschaft Wissen schafft: Wissenschaftstheorie und-ethik für die Sozial-und Wirtschaftswissenschaften. UTB: Stuttgart
- Theisen, M. R. & Theisen, M. (2013). Wissenschaftliches Arbeiten: Erfolgreich bei Bachelor- und Masterarbeit; [das Standardwerk neu konzipiert (16., vollst. überarb. Aufl.). Vahlen: München.
- Wiltinger, K. & Wiltinger, A. (2014). Wissenschaftliches Arbeiten: Praxisleitfaden für Studierende. Cuvillier: Göttingen
- Wissenschaftliche Paper zur gewählten Forschungsfrage

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

SCHWERPUNKT III: Kryptografie

SPIII-1 Einführung in die Kryptografie

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden verstehen die mathematischen Grundlagen der Kryptographie.
- Sie verstehen die Prinzipien von Public und Secret-Key-Verschlüsselung sowie der relevanten Verfahren einschließlich ihrer Sicherheit und Effizienz.
- Die Studierenden kennen die Prinzipien digitaler Signaturen und der relevanten Verfahren einschließlich ihre Sicherheit und Effizienz.
- Die Studierenden kennen die grundlegenden symmetrischen Verschlüsselungssystemen in der Praxis, sowie die Grundlagen der asymmetrischen Kryptographie insbesondere das weitverbreitete RSA-Krypto-sys-tem und die wichtigsten Ersätze der asymmetrischen Methoden (Diffie-Hellman und elliptische Kurven).
- Sie können die Grundlagen den Quantenkryptografie erklären.

Inhalte

- Mathematische Grundlagen:
  Berechnungen in Kongruenz- und Restklassenringen; Faktorisierung großer Zahlen; Wahrscheinlichkeit; Modulare Arithmetik; Euklidischer Algorithmus; Endliche Felder; Faktorisierung großer Zahlen; Diskrete Logarithmen; Chinesischer Restsatz; Quadratischer Rest; Elliptische Kurven
- Grundlagen der Verschlüsselung:
  Geschichte der Kryptologie; Symmetrische vs. Asymmetrische Kryptosysteme; Block- und Stromchiffren; Kryptanalyse; Verschlüsselung mit öffentlichen Schlüsseln; RSA, Diffie-Hellman, ElGamal; Message Authentication Codes bzw.kryptographische Prüfsummen; Digitale Signaturen; Identifikation; Monoalphabetische Substitution; Struktur des Restklassenrings Z/mZ; Randomisierte Homophonie; Vigenere-Verschlüsselung, Kappa- und Phi-Index; Zweifache klassische Vigenere-Verschlüsselung; Zylinder und Rotoren; Vernam-Chiffrierung, One-Time-Pad; Pseudo-Zufalls-Generatoren; Data-Encryption-Standard (DES); Advanced-Encryption-Standard (AES); IDEA-Algorithmus; Huffman-Codes; Lempel-Ziv-Kompression; Kryptographie-Verfahren; Primzahltests; Faktorisierungs-Algorithmen; Message Digests, RSA-Signatur; RC5-Algorithmus, RSA-Challenge 1997; Diffie-Hellman Schlüssel-Vereinbarung; ElGamal-Signatur, DSS (Digital Signature Standard)

Empfohlene Voraussetzungen für die Teilnahme:
keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Buchmann, J. (2010). *Einführung in die Kryptographie* (5. Aufl.). Springer.
- Paar, C. & Pelzl, J. (2016). *Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender*. Springer Vieweg.
- Rogaway, P. & Bellare, M. (2005). *Introduction to Modern Cryptography*. Lecture Notes. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf
- Buchmann, J. (2010). *Einführung in die Kryptographie* (5. Aufl.). Springer.
- Schneier, B. (2015). *Secrets and Lies: Digital Security in a Networked World*. Wiley.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

Klausur (120 Minuten) (100%)

SPIII-2 Angewandte Kryptografie

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die Grundbegriffe, Ziele und grundlegende Methoden der modernen Kryptographie.
- Sie verstehen die Arbeitsweise, Sicherheitsvoraussetzungen sowie Einsatzmöglichkeiten einiger aktueller kryptographischer Verfahren.
- Die Studierenden können die Sicherheitsanforderungen eines gegebenen Anwendungsszenarios analysieren und die Eignung verschiedener kryptographischer Verfahren dafür bewerten.
- Sie sind in der Lage, für eine Anwendung geeignete kryptographische Verfahren und Werkzeuge auszuwählen, diese Auswahl mit fundierten Fachkenntnissen zu begründen sowie die Verfahren bzw. Werkzeuge in der Praxis fachgerecht einzusetzen.
- Sie können Sicherheitslösungen in Unternehmen basierend auf Konzepten der symmetrischen und asymmetrischen Kryptographie (PKI, di-gi-tale Zertifizierungen, usw.) anwenden.
- Die Studierenden verstehen die Anwendungen der Kryptographie an ausgewählten use cases, wie zum Beispiel Mobiltelefonie oder der Durchführung elektronischer Wahlverfahren.

Inhalte

- Authentifizierte Verschlüsselung und ihre symmetrische Stammfunktionen (inkl. AES-GCM, AES-CCM, …)
- Kryptographische Hashfunktionen und ihre Stammfunktionen (incl. SHA-2, SHA-3)
- Asymmetrische Verschlüsselung und Schlüssel-Kapselung, (incl. RSA, DH, DSA, ECC)
- Authentifizierung und Schlüsselaustauschprotokolle, inklusive eine Einführung in die fortgeschrittene privacy-preserving Protokolle
- Quantenkryptographie und Post-Quantenkryptographie
- Elliptische Verschlüsselungsverfahren
- Einfache Chiffrierverfahren (Substitution und Transposition)
- Boolesche Funktionen mit Anwendungen in der Kryptographie
- Schlüsselaustausch, z.B. Diffie-Hellman
- Symmetrische Kryptosysteme: Arbeitsweise und Einsatz am Beispiel von AES, Betriebsarten
- Asymmetrische Kryptosysteme: Arbeitsweise und Einsatz am Beispiel von RSA
- PKI, digitale Zertifizierungen, Digitale Signaturen auf Zertifikate
- Ausarbeitung kryptographischer Protokolle zur sicheren Datenübertragung (z.B. TLS, SSH)

Voraussetzungen für die Teilnahme
keine

Verwendbarkeit
- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: Lab
virtuelle Lehrveranstaltungen mit optionalen Präsenzveranstaltungen mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativen Lernen
- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Übungen auf der Online-Lernplattform (z.B. Quizzes, individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Eckert, C. (2018). *IT-Sicherheit*. De Gruyter.
- Daemen, J. & Rijmen, V. (2002). *The Design of RijndaeL: AES - The Advanced Encryption Standard*. Springer.
- Mollin, R. A. (2005). *Codes: The Guide to Secrecy From Ancient to Modern Times*. Chapman and Hall/CRC.
- Stinson, D. R. (2005). *Cryptography: Theory and Practice*. Chapman and Hall/CRC.
- Wagstaff, S. S. (2003). *Cryptanalysis of Number Theoretic Ciphers*. CRC Press.
- Aumasson, J. (2017). *Serious Cryptography: A Practical Introduction to Modern Encryption*. No Starch Press.
- Paar, C. & Pelzl, J. (2016). *Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender*. Springer Vieweg.
- Schmeh, K. (2016). *Kryptografie: Verfahren, Protokolle, Infrastrukturen*. Dpunkt.Verlag GmbH.
- Schwenk, J. (2014). *Sicherheit und Kryptographie im Internet* (4. Aufl.). Springer Vieweg.
- Wätjen, D. (2018). *Kryptographie: Grundlagen, Algorithmen, Protokolle* (3. Aufl.). Springer Vieweg.
- Brands, G. (2011). *Einführung in die Quanteninformatik: Quantenkryptografie, Teleportation und Quantencomputing*. Springer.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
- Studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)

SPIII-3 Forschungsprojekt

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden sind in der Lage, wissenschaftliche Fragestellungen und Hypothesen zu formulieren.
- Sie können geeignete wissenschaftliche Publikationen auswählen und verstehen.
- Sie verstehen den Einsatz empirischer Methoden zur Erlangung wissenschaftlicher Erkenntnisse und können diese anwenden. Sie können Forschungsmethoden zur Beantwortung wissenschaftlicher Hypothesen kritisch reflektieren.
- Sind in der Lage, Ergebnisse von empirischen Forschungsprozessen korrekt zu interpretieren, darzustellen und kritisch zu reflektieren.
- Die Studierenden sind in der Lage, effektiv in remoten Arbeitsgruppen an einem gemeinsamen Projekt zu arbeiten.

Inhalte

- Entwicklung einer Forschungsfrage mit thematischem Bezug zum Schwerpunkt
- Durchführung einer Literaturrecherche und Aufbereitung des aktuellen Forschungsstandes zur Forschungsfrage
- Formulierung von Hypothesen auf Basis einer gewählten Bezugstheorie bzw. des aktuellen Forschungstandes
- Wahl und Durchführung einer geeigneten empirischen Methode zur Überprüfung der Hypothesen inkl. Operationalisierung der relevanten Konstrukte, Erhebung von Primärdaten oder Recherche von Sekundärdaten sowie Datenauswertung
- Interpretation und kritische Reflexion der Ergebnisse
- Ableitung wissenschaftlicher und praktischer Implikationen
- Dokumentation des gesamten Forschungsprojekts in einer Projektarbeit
- Vorbereitung und Durchführung einer wissenschaftlichen Präsentation der Ergebnisse

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Data Science & Management (M.Sc.)
- Cybersecurity & Privacy (M.Sc.)

- Digital Responsible Leadership (M.Sc.)

Lehr- und Lernformen: Projekt
virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf problemorientiertem Lernen anhand eines konkreten realen oder fiktiven Projektauftrages

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Übungen auf der Online-Lernplattform (z.B. Quizzes, individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten
- Projektarbeit in (virtuellen) Teams

Basisliteratur

- Backhaus, K. Erichson, B., Plinke, W. & Weiber, R. (1994). Multivariate Analysemethoden. Eine anwendungsorientierte Einführung (11. Überarbeitete Auflage). Berlin: Springer.
- Baur, N. & Blasius, J. (2019). Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer Vieweg.
- Brühl, R. (2017). Wie Wissenschaft Wissen schafft: Wissenschaftstheorie und-ethik für die Sozial-und Wirtschaftswissenschaften. UTB: Stuttgart
- Theisen, M. R. & Theisen, M. (2013). Wissenschaftliches Arbeiten: Erfolgreich bei Bachelor- und Masterarbeit; [das Standardwerk neu konzipiert (16., vollst. überarb. Aufl.). Vahlen: München.
- Wiltinger, K. & Wiltinger, A. (2014). Wissenschaftliches Arbeiten: Praxisleitfaden für Studierende. Cuvillier: Göttingen
- Wissenschaftliche Paper zur gewählten Forschungsfrage

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

Wahlpflichmodule WP (Auszug)

WP Einführung Künstliche Intelligenz

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen grundlegende Begriffsdefinitionen und sind mit den Grundsätzen zum Themenkomplex „Künstliche Intelligenz“ sowie mit den grundlegenden Konzepten vertraut.
- Sie verstehen die Prinzipien von algorithmischen Suchverfahren sowie agentenbasierten Systemen.
- Die Studierenden verstehen die Grundlagen und Konzepte des maschinellen Lernens und verwandter Themen
- Sie kennen verschiedene Anwendungsbereiche der Künstlichen Intelligenz und die damit verbundene Chancen und Risiken.
- Die Studierenden sind sich möglicher, zukünftiger Entwicklungen im Bereich Künstliche Intelligenz bewusst und sind in der Lage, aktuelle und zukünftige Entwicklungen vor dem Hintergrund ethischer Fragenstellungen kritisch zu reflektieren.

Inhalte

- Einführung in die Grundbegriffe der künstlichen Intelligenz
- Historischer Entwicklungen der KI (technologische Entwicklungen, aktuelle Fortschritte)
- Wissensrepräsentationen (Ontologies)
- Algorithmische Entscheidungsfindung und KI in der Programmierung
- Agentenbasierte Modellierung
- Suchverfahren (Informierte und uninformierte Suchverfahren), adversariale Suche
- Maschinelles Lernen
- Neuronale Netze, Evolutionäre Algorithmen
- Künstliche Intelligenz in Industrie und Gesellschaft
- Zukünftige Entwicklungen und ethische Fragestellungen

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Digital Responsible Leadership (M.Sc.)
- Data Science & Management (M.Sc.)
- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Buxmann, P. & Schmidt, H. (2019). *Künstliche Intelligenz. Mit Algorithmen zum wirtschaftlichen Erfolg*. Berlin: Springer Gabler.
- Gröner, S. & Heinecke, S. (2019). *Kollege KI. Künstliche Intelligenz verstehen und sinnvoll im Unternehmen einsetzen*. München: Redline Verlag.
- Kreutzer, R. T. & Sirrenberg, M. (2019). *Künstliche Intelligenz verstehen. Grundlage – Use-Cases – unternehmenseigene KI-Journey*. Wiesbaden: Springer Gabler.
- Michalski, R. S., Carbonell, J. G. & Mitchell, T. M. (2013). *Machine Learning, An Artificial Intelligence Approach*. Springer.
- Retti, J., Bibel, W., Buchberger, B., Buchberger, E., Horn, W., Kobsa, A., Steinacker, I., Trappl, R. & Trost, H. (2014). *Artificial Intelligence — Eine Einführung*. Vieweg+Teubner Verlag.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienbegleitende Leistungsnachweise (100%)

WP Cybersecurity in Operational Technology

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen den grundsätzlichen Aufbau von Operational Technology Umgebungen sowie die Funktionsweise unterschiedlicher Sensoren und Aktoren.
- Die Studierenden sind in der Lage, unterschiedliche Angriffsvektoren auf OT Systeme zu benennen, zu identifizieren und Gegenmaßnahmen zu beschreiben.
- Sie können die Konvergenz zwischen IT und OT beschreiben und elementare Schutzmaßnahmen beider Systemwelten an ihren Übergängen definieren, einrichten und betreiben.
- Die Studierenden kennen die Besonderheiten von IP Protokollen und Anwendungsprotokollen und können deren Bedeutung für die Sicherheit einschätzen.
- Die Studierenden kennen die Rahmenbedingung für den Betrieb von OT Umgebungen, welche i.d.R. den Auflagen der Hersteller unterliegen. Sie können sie im Rahmen von mitigierenden Sicherheitsmaßnahmen erkennen und behandeln.

Inhalte

- Aufbau von SCADA und ICS Systeme
- Aufbau von Gebäudeautomationssysteme, wie KNX
- Abgrenzung von IoT Systemen zu IT Systemen und zu OT Systemen
- Aufbau des Protokollstacks für OT / IoT Systeme
- Betriebsbedingungen von OT Systemen
- Typische Sicherheitsmaßnahmen für OT Umgebungen
- Sicherheitsaspekte von Remote Wartungszugängen

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Fournaris, A. P., Lampropoulos, K. & Tordera, M. E. (2019). *Information and Operational Technology Security Systems: First International Workshop, IOSec 2018, CIPSEC Project*. Springer.
- Blokdyk, G. (2019). *Operational Technology Security A Complete Guide*. Emereo Pty Limited.
- Bodungen, C., Singer, B., Shbeeb, A., Wilhoit, K. & Hilt, S. (2016). *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions*. McGraw-Hill Education.
- Colbert, E. J. M. & Kott, A. (2016). *Cyber-security of SCADA and Other Industrial Control Systems*. Springer.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

- Studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)

WP Cyber Resilience

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden verstehen den Begriff Cyber Resilience in der Theorie und können ihn zum klassischen Sicherheitsbegriff abgrenzen.
- Sie können Cyber Resilience unter wissenschaftlichen Gesichtspunkten diskutieren und Aspekte wie Vulnerabilität, Coping Capacities und Robustheit zueinander in Bezug setzen.
- Sie sind in der Lage, Cyber Resilience in anwendungsorientierte Konzepte zu übertragen.
- Sie kennen die wesentlichen Quellen und Institutionen zum Thema Cyber Resilience.

Inhalte

- Einführung Systemtheorie
  - Grundbegriffe und Konzepte
  - Interdisziplinäre Forschungsrichtungen
- Abstrakte Betrachtung Cyber Security
  - Grundannahmen
  - Technische und organisatorische Maßnahmen
- Abstrakte Betrachtung Cyber Resilience
  - Grundannahmen
  - Gefahr, Exposition, Vulnerabilität, Coping Capacity, Adaptability
- Anwendungsorientierte Betrachtung Cyber Resilience
- Organisationstheorie
- Changemanagement
- Messbarkeit von organisationalen Fähigkeiten

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cybersecurity & Privacy (M.Sc.)
- Data Science & Management (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform

- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Gallopin, G. C. (2006). *Linkages between Vulnerability, Resilience, and Adaptive Capacity. Global Environmental Change. pp. 293–303*.
- Reason, J. (2000). *Safety Paradoxes and Safety Culture. Injury Control and Safety*. pp. 3-14. Taylor & Francis Online.
- Kott, A. & Linkov, I. (2018). *Cyber Resilience of Systems and Networks (Risk, Systems and Decisions)*. Springer.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

- Studienbegleitende Leistungsnachweise 40%
- Studienarbeit 60%

WP Design Thinking Methods: Product Development & Service Design

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Studierende kennen Grundlagen und wichtige Methoden des Design Thinking-Ansatzes und können diese zur Entwicklung von Produkten oder Dienstleistungen anwenden.
- Sie sind mit wichtigen Phasen des Design Thinking-Prozesses vertraut und können diese selbständig planen, organisieren und durchführen.
- Studierende verstehen die Besonderheiten digitaler Produkte und Dienstleistungen und können diese bei deren Entwicklung und Gestaltung berücksichtigen.

Inhalte

- Grundlagen und Methoden des Design Thinking, u.a.
  - User Research und Personas
  - Customer Journey und Touchpoints
  - Kreativitätstechniken
  - Rapid Prototyping
  - Storyboarding
  - Testmethoden
- Phasen des Design Thinking Prozesses
  - Problemdefinition und -analyse
  - Beobachtung
  - Synthese
  - Ideation
  - Prototyping
  - Testen
- Besonderheit digitaler Produkte und Services, u.a.
  - User Experience Design
  - Lock in-Effekte
  - Datengetriebene Produkte und Services
  - Produkt-Service-Bündel
  - User-Driven Innovation und Co-Creation

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Digital Responsible Leadership (M.Sc.)

- Data Science & Management (M.Sc.)
- Cybersecurity & Privacy (M.Sc.)

Lehr- und Lernformen: Lab
virtuelle Lehrveranstaltungen mit optionalen Präsenzveranstaltungen mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativen Lernen

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Übungen auf der Online-Lernplattform (z.B. Quizzes, individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Lewrik, M., Link, P., Leifer, L. (Hrsg.) (2018). *Das Design Thinking Playbook*. 2. Aufl. München: Vahlen.
- Lewrik, M., Link, P., Leifer, L. (Hrsg.) (2018). *Das Design Thinking Toolbook*. München: Vahlen.
- Pioch, S. (2019). *Digital Entrepreneurship. Ein Praxisleitfaden für die Entwicklung eines digitalen Produkts von der Idee bis zur Markteinführung.* Wiesbaden: Springer Gabler
- Schallmo, D. R. A., Lang, K. (2020). Design Thinking erfolgreich anwenden. 2. Aufl. Wiesbaden: SpringerGabler.
- Schrader, Matthias (2017). *Transformationale Produkte. Der Code von digitalen Produkten, die unseren Alltag erobern und die Wirtschaft revolutionieren.* Hamburg: Next Factory Ottensen
- Stich, V. et al. (Hrsg.) (2019). *Digitale Dienstleistungsinnovationen: Smart Services agil und kundenorientiert entwickeln.* Wiesbaden: Springer Vieweg

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)

- studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)