Digital Business University of Applied Sciences

Cyber- & IT-Security (M.Sc.)

Modulhandbuch

Version: 06.2023

I. Vorwort

Der Masterstudiengang Cyber- & IT-Security (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 Modulen 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 dabei oberstes Gebot. In Zeiten immer stärkerer IT-Vernetzung, auch auf globaler Ebene, bedarf es eines qualifizierten Nachwuchses, der Unternehmen dabei unterstützt, den Bereich der Cyber- & IT-Security umfassend zu betrachten. IT-Sicherheit ist daher ein zentrales Thema, denn der Schutz von IT-Systemen hilft, Risiken wie z.B. Hackerangriffe abzuwehren und somit möglichen finanziellen wie Image-Schäden vorzubeugen.

Der Masterstudiengang Cyber- & IT-Security (M.Sc.) hat sich die Ausbildung von Expert:innen zum Ziel gesetzt, die leitende, beratende oder selbständige Tätigkeiten im Bereich der Cyber- & IT-Security übernehmen. Der Studiengang fokussiert dabei auf den Bereich der Informationstechnik und dessen Sicherheit. Im Vordergrund stehen vor allem technik-orientierte Aspekte wie z.B. Security Engineering und Netzwerksicherheit.

Nach dem Studium bieten sich den Absolvent:innen mit dem in diesem Masterstudiengang erworbenen Kompetenzen zahlreiche Möglichkeiten für einen Karriereeinstieg oder -aufstieg in Cyber- & IT-Security-Bereiche.

Absolvent:innen des Masterstudiengangs Cyber- & IT-Security (M.Sc.) sind unter anderem in folgenden Positionen tätig:

- Unternehmensberater:in Informationssicherheit
- Enterprise Security Architect
- Schwachstellenanalytiker
- Malware-Analyst
- Business Continuity Manager
- IT-Forensiker
- Mitarbeiter in Cybersecurity Projekten

III. Studienziel

Der Studiengang Cyber- & IT-Security (M.Sc.) qualifiziert Absolvent:innen vor allem in technischen Gesichtspunkten der IT-Sicherheit. Das Verständnis von unterschiedlichen Aspekten der IT-Sicherheit bereitet ideal auf eine verantwortungsvolle Übernahme künftiger Aufgaben in der IT-Sicherheit vor.

Der Studiengang vermittelt sowohl eine umfassende wissenschaftliche als auch eine praxisorientierte Ausbildung. Studierende haben zudem die Möglichkeit, ihr Studium durch Schwerpunkte in den folgenden Bereichen zu ergänzen:

- Informatik für Cyber- & IT-Security
- Tools & Applications in Cyber- & IT-Security
- Cyber Security Management

Absolvent:innen wird in diesem Studiengang fachliches Wissen vermittelt, welches für die Einrichtung und den Betrieb sicherer IT-Systeme benötigt wird. Sie kennen technische Verfahren zur Erreichung von IT-Sicherheit und können diese anwenden. Dies beinhaltet unter anderem IT-Systeme hinsichtlich ihrer Sicherheit zu analysieren, dabei mögliche Schwachstellen aufzuzeigen und Vorschläge zu unterbreiten, wie diese zu beheben sind.

Neben breitem Fachwissen wird vor allem auch Methodenkompetenz vermittelt. Diese erlaubt es Studierenden, komplexe Projekte der Cyber- & IT-Sicherheit selbstständig, verantwortungsbewusst und strukturiert umzusetzen. Dies beinhaltet z.B. die Klassifizierung von Sicherheitsproblemen, die strukturierte Analyse IT-forensischer Vorgänge sowie eine Bewertung von Angriffsmechanismen und Gegenstrategien. Darüber hinaus sind Absolvent:innen in der Lage, neueste Erkenntnisse der Cyber- & IT-Security, Methoden und Anwendungsapplikationen kritisch zu evaluieren.

Ergänzend werden im Studiengang Cyber- & IT-Security (M.Sc.) auch modulübergreifende soziale und Selbstkompetenzen vermittelt. Absolvent:innen werden somit in die Lage versetzt, ihr Fachwissen auch im Kontext gemeinsamer Zusammenarbeit, z.B. mit anderen Cyber- & IT-Security Spezialisten oder Abteilungen, anzuwenden und letztlich Cyber- & IT-Security auch als Teamarbeit zu verstehen. Dies beinhaltet auch eine kritische Reflexion der eigenen Fähigkeiten.

Der Masterstudiengang eignet sich für Absolvent:innen mit einem ersten berufsqualifizierenden Hochschulabschluss (Bachelorabschluss), vorzugsweise der (Wirtschafts-)Informatik oder aus dem Bereich der Wirtschafts-, Rechts- oder Ingenieurwissenschaften. Der Studiengang richtet sich an Berufstätige unterschiedlichster Branchen- und Berufshintergründe, die ihr Wissen im Bereich Cyber- & IT-Security aufbauen und erweitern möchten.

IV. Übersicht über Module und Leistungsnachweise

vgl. Anlage 1 Studien- und Prüfungsordnung

Lfd. NR	Modul	Art der Lehrver-anstal-tung	Zugangs-voraus-set-zung	Art der Prüfungs-leistung	ECTS-Kredit-punkte
(PLAN-)SEMESTER 1					
01	Grundlagen Cyber- und IT-Security	SK	Keine	K (120)	6
02	Informationstechnik für Cyber- & IT-Security	SK	Keine	SL	6
03	Network Security	SK	Keine	SL	6
04	Systemanalyse	SK	Keine	ST	6
05	Cloud Computing & Cloud Security	SK	02	ST	6
(PLAN-)SEMESTER 2					
06	Cyber Resilience	SK	Keine	SL/ST	6
07	Telekommunikations- und Kommunikationstechnologien	SK	Keine	K (120)	6
08	Schwerpunktmodul 1	s.u.	s.u.	s.u.	s.u.
09	Datenmodellierung und Datenbanksysteme	SK	Keine	K (120)	6
10	Cyber- & IT-Security: Implementation & Application	SK	Keine	ST	6
(PLAN-)SEMESTER 3					
11	Wahlpflichtmodul	s.u.	s.u.	s.u.	s.u.
12	Advanced Research Methods	SK	Keine	SL/ST	6
13	Cyber- IT-Forensik	SK	Keine	ST	6
14	Schwerpunktmodul 2	s.u.	s.u.	s.u.	s.u.
15	Schwerpunktmodul 3 - Forschungsprojekt	s.u.	s.u.	s.u.	s.u.
(PLAN-)SEMESTER 4					
16	Kolloquium & Schreibwerkstatt	L	Keine	uSL	6
17	Masterarbeit	M	Anmeldung 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
uSL	unbenotete Studienleistung

SCHWERPUNKTE
wählbare Schwerpunkte und Module im Studiengang Cyber- & IT-Security (M.Sc.)
vgl. Anlage 2 Studien- und Prüfungsordnung

Lfd. NR	Modul	Art der Lehr-veran-staltung	Zugangs-voraus-setzung	Art der Prüfungs-leistung	ECTS-Kredit-punkte
SCHWERPUNKT I: Informatik für Cyber- & IT-Security					
SPI-1	Informatik für Cyber Security I	SK	Keine	SL/ST	6
SPI-2	Informatik für Cyber Security II	SK	Keine	SL	6
SPI-3	Forschungsprojekt	PR	Keine	SL	6
SCHWERPUNKT II: Tools & Applications in Cyber- & IT-Security					
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: Cybersecurity Management					
SPIII-1	Managementsysteme und In-foSec-Standards	SK	Keine	K (120)	6
SPIII-2	Grundlagen von Audits, Reviews und Assessments	SK	Keine	K (120)	6
SPIII-3	Forschungsprojekt	PR	Keine	SL	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
uSL unbenotete Studienleistung

WAHLPFLICHTMODULE
mögliche Wahlpflichtmodule im Studiengang Cyber- & IT-Security (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	Systemsicherheit	SK	Keine	SL	6
WP2	Cybersecurity in Operational Tech-nology	SK	Keine	SL/ST	6
WP3	Agiles Projektmanagement	SK	Keine	SL/ST	6
WP4	Public-Key-Infrastructure	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
uSL unbenotete Studienleistung

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 Grundlagen Cyber- und IT-Security

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 haben ein fundiertes Verständnis von Netzwerkarchitekturen und -protokollen sowie von Techniken zum Schutz von Netzwerken vor Angriffen.
- Sie können Sicherheitsmaßnahmen für Rechner und Netzwerkgeräte, wie z.B. Firewalls, Anti-Virus-Software und Verschlüsselung, einsetzen und verwalten.
- Sie haben ein Verständnis für die Sicherheit von Anwendungen, insbesondere von Web-Anwendungen, und die Vermeidung von OWASP Sicherheitsrisiken.

Inhalte

- Angriffs- und Schutzmethoden
- Netzwerksicherheit und Firewalls
- Kryptographie und Verschlüsselungstechnologien
- IT-Forensik und Incident Response
- Cloud-Sicherheit und Cyber-Geopolitik
- Sicherheit von IoT- und mobile Geräten

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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.
- Information Resources Management Association. (2019). Cloud Security: Concepts, Methodologies, Tools, and Applications. IGI Global

- Dotson, C. (2019). Practical Cloud Security: A Guide for Secure Design and Deployment. O'Reilly Media

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

02 Informationstechnik für Cyber- & IT-Security

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 haben vertiefte Kenntnisse im Umgang mit Informationstechnik, IT-Security-Tools und -Technologien.
- Sie können Sicherheitsmaßnahmen in der IT-Infrastruktur zielgerichtet anwenden.
- Sie verstehen Angriffstechniken und -methoden und können deren Eignung und Folgen auf Informationstechnologien beurteilen.
- Sie kennen Methoden zur Identifizierung, Bewertung und Behebung von IT-Sicherheitsrisiken in Informationstechnologien und können diese anwenden.

Inhalte

- Rechnerarchitekturen und Komponenten
- Verteilte Systeme, Netzwerke und Netzwerk-Technologien
- IoT-Geräte
- Übertragungstechnik und -Mechanismen

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Bühler, P., Schlaich, P., Sinner, D. (2018). Informationstechnik: Hardware – Software – Netzwerke. Springer Verlag
- Schiemann, B., Grimm, B., Vogler, H., Troßmann, H., Dehler, E., Philipp, W., Häberle, G., Schmid, D. (2011) Informations- und Kommunikationstechnik. Europa-Lehrmittel

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

03 Network Security

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 relevante Netzwerksicherheitstechnologien und -protokolle.
- Sie können Netzwerksicherheitsrisiken identifizieren und bewerten sowie Netzwerksicherheitsmaßnahmen planen, implementieren und überwachen.
- Sie können Zugriffskontrollen und Authentifizierungsmechanismen implementieren.
- Sie kennen relevante Firewall-Technologien, -designs und -konfigurationen.
- Sie können Netzwerksicherheitsvorfälle erkennen, analysieren und beheben.

Inhalte

- Grundlagen der Netzwerksicherheit: Verschlüsselung, Authentifizierung, Zugriffssteuerung
- Cloud-Sicherheit und Sicherheit in virtualisierten Umgebungen
- Angriffsmethoden und Schutzmaßnahmen
- Public Key Infrastrukturen (PKI)
- Secure Socket Layer (SSL) und Transport Layer Security (TLS)
- Firewall-Technologien, -Design und -konfigurationen
- Virtual Private Networks (VPN)

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Gert, D., Gert, S. Network Security Fundamentals (2005). Cisco Press

- McNab, C. Network Security Assessment: Know Your Network (2016). O'Reilly Media
- Stallings, W. Cryptography and Network Security: Principles and Practice (2016). Pearson EDUC

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

04 Systemanalyse

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 wichtigsten Angriffstechniken und Abwehrmaßnahmen sowie Sicherheitsarchitekturen und -konzepte.
- Sie verstehen methodische Ansätze zur Analyse von IT-Systemen.
- Sie können IT-Systeme auf Schwachstellen und Risiken hin untersuchen.

Inhalte

- Einführung in die Systemanalyse
- Anforderungsmanagement
- Funktions- und Leistungsanalyse
- Systems Engineering und Modellierungstechniken
- Aspektorientierte Modellierung

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Dennis, A., Wixom, B., Roth, R. Systems Analysis and Design, 5th Edition (2012). John Wiley & Sons
- Sajja, P. Essence of Systems Analysis and Design (2017). Springer
- Heinrich, G. Allgemeine Systemanalyse (2007). Oldenbourg Wissenschaftsverlag

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

Studienarbeit (100%)

05 Cloud Computing & Cloud Security

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 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

Modul 02

Verwendbarkeit

- Cyber- & IT-Security (M.Sc.)
- Cybersecurity & Management (MBA)

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)
Studienarbeit (100%)

06 Cyber Resilience

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 sind in der Lage, die Widerstandsfähigkeit von IT-Systemen und -Netzwerken gegen Cyberangriffe zu erhöhen.
- Sie können Prozesse und Verfahren zur regelmäßigen Überwachung und Verbesserung der IT-Security implementieren.
- Sie können Angriffe auf IT-Systeme und Netzwerke erkennen und angemessen reagieren.
- Sie können die Auswirkungen von erfolgreichen Angriffen auf IT-Systeme minimieren.

Inhalte

- Identifizierung und Bewertung von Risiken und Bedrohungen im Cyberraum
- Schutz von IT-Systemen und Daten durch proaktive Maßnahmen
- Implementierung von Notfallplänen und Business Continuity Management
- Regelmäßige Überwachung und Überprüfung der IT-Security
- Modelle der Zusammenarbeit mit Partnern und Dienstleistern für die Optimierung der Cyber Resilience
- Erstellung von Berichten und Statistiken zur Überwachung des Sicherheitsstatus

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (M.Sc.)
- Cybersecurity & Management (MBA)

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

- Petrenko, S. Cyber Resilience (2019). River Publishers

- Axelos. Cyber Resilience Best Practices (2015). The Stationery Office Ltd
- Linkov, I., Kott, A. Cyber Resilience of Systems and Networks (2018). Springer

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

07 Telekommunikations- und Kommunikationstechnologien

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 fundiertes Fachwissen in den Bereichen Telekommunikation und Kommunikationstechnologien.
- Sie verstehen die grundlegenden Konzepte und Technologien der digitalen Kommunikation.
- Sie können Telekommunikationssysteme entwerfen, implementieren und sicher betreiben.
- Sie können komplexe technische Probleme im Bereich Telekommunikations- und Kommunikationstechnologien analysieren und lösen.

Inhalte

- Grundlagen der Telekommunikation, Signalübertragung, Modulation, Multiplexing
- Netzwerktechnologien, Routing, Switching
- Drahtlose Kommunikation, WLAN, Bluetooth, Mobile Kommunikation
- Datenübertragungstechnologien, DSL, Fiber Optik, 5G
- Medientechnologien, Streaming, VoIP, IP-Telefonie
- Regulierung und Standards in der Telekommunikation
- Netzwerkdesign, Implementierung von Kommunikationssystemen

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Conrads, D. Telekommunikation: Grundlagen, Verfahren, Netze (2004). Vieweg Friedr. + Sohn Verlag
- Neumann, A. Telekommunikationsrecht kompakt (2021). Fachmedien Recht und Wirtschaft in Deutscher Fachverlag GmbH
- Fitzgerald, J., Dennis, A., Durcikova, A. Business Data Communications and Networking (2020). Wiley / Wiley & Sons

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Klausur (120 Minuten) (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 Datenmodellierung und Datenbanksysteme

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 entwickeln ein Verständnis für die Konzepte und Methoden der Datenmodellierung und des Datenbankdesigns.
- Sie kennen verschiedene Datenbankmodelle und können deren Einsatzmöglichkeiten evaluieren.
- Sie können Datenanalyse- und -abfragetechniken anwenden, um Daten aus Datenbanken zu extrahieren.
- Sie kennen die Anforderungen an Datensicherheit in Bezug auf Datenbanken.
- Sie können Datenbanken über geeignete Techniken und Methoden, wie z.B. Verschlüsselung und Zugriffskontrolle, absichern.

Inhalte

- Grundlagen der Datenmodellierung für relationaler und NoSQL Datenbanken
- Konzeption und Design von Datenbanken
- Sicherheitstechniken für Datenbanken, Zugriffssteuerung, Verschlüsselung
- Anwendung von Datenbankmanagementsystemen (DBMS)
- Verwendung von SQL für die Datenmanipulation
- Konzeption und Implementierung von Datenbanksystemen in einem sicheren IT-Umfeld
- Anwendung von Datenbanken in der IT-Security

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Garcia-Molina, H., Ullman, J., Widom, J. Database Systems: The Complete Book (2008). Prentice Hall
- Hoberman, S. Data Modeling Made Simple: A Practical Guide for Business and IT Professionals, 2nd Edition (2015). Technics Publications
- Wagner, Dominik. Sicherheit in DBMS (2011). Grin Verlag

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

10 Cyber- & IT-Security: Implementation & Application

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

- Verständnis der Grundlagen von IT-Security, z.B. Kryptografie, Netzwerksicherheit, Anwendungssicherheit
- Kompetenzen in der Implementierung von IT-Security-Maßnahmen
- Fähigkeit, IT-Security-Risiken zu erkennen und zu bewerten
- Kenntnisse über Compliance-Anforderungen und -Standards, z.B. ISO 27001
- Fähigkeit, IT-Security-Maßnahmen in Unternehmensprozesse zu integrieren
- Verständnis der rechtlichen Aspekte von IT-Security, z.B. Datenschutz, Computer-strafrecht
- Fähigkeit, IT-Security-Audits begleiten und IT-Security-Pläne zu erstellen
- Security Information and Event Management (SIEM)

Inhalte

- Sicherheit von Betriebssystemen und Anwendungen
- Kryptographie und Verschlüsselungstechnologien
- Identitäts- und Zugriffsmanagement
- Compliance und Datenschutzgesetze
- Disaster Recovery und Business Continuity Management
- Sicherheit in Cloud-Computing-Umgebungen
- Sicherheit im Internet of Things (IoT)
- Management von IT-Sicherheitsrisiken und -Governance
- Projektmanagement und Implementierung von IT-Sicherheitsmaßnahmen

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Miller, D., Harris, S., Harper, A., VanDyke, S., Blask, C. Security Information and Event Management (SIEM) Implementation (2010). McGraw Hill
- Bishop, M. Computer Security: Art and Science (2018). Pearson Education
- Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)
Studienarbeit (100%)

11 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

12 Advanced Research Methods

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 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.)
- Cyber- & IT-Security (M.Sc.)
- Digital Responsible Leadership (MBA)
- Corporate Entrepreneurship & Innovation (MBA)
- Digital Strategy & Data Management (MBA)

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 Sozialfor- schung. 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%)

13 Cyber- & IT-Forensik

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 grundlegenden Konzepte der Cyber- und IT-Forensik.
- Sie können relevante Methoden und Techniken zur Untersuchung von Cyber-Verbrechen und IT-Sicherheitsvorfällen anwenden.
- Sie kennen die gängigen Forensik-Tools und -Software.
- Sie können IT-forensische Untersuchungen durchführen und zugehörige Berichte erstellen.
- Sie haben ein Verständnis der rechtlichen Aspekte der Cyber-Forensik und IT-Forensik.
- Sie können mit anderen Abteilungen wie dem IT-Sicherheitsteam und Strafverfolgungsbehörden zusammenarbeiten.

Inhalte

- Untersuchung und Analyse von digitalen Spuren in Computersystemen und Netzwerken
- Wiederherstellung gelöschter Daten und Dateien
- Beweissicherung und -präsentation in gerichtlichen Verfahren
- Kenntnisse in verschiedenen Betriebssystemen, Netzwerken, Programmiersprachen
- Kenntnisse in verschiedenen Forensik-Tools und -Methoden

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Sachowski, J. Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise (2018). Taylor & Francis Ltd
- EC-Council. Computer Forensics: Investigating Network Intrusions and Cybercrime (CHFI), 2nd Edition (2016). Cengage Learning
- Gogolin, G. Digital Forensics Explained (2021). CRC Press

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

14 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

15 Schwerpunktmodul 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

Siehe Beschreibung der Schwerpunktmodule

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.)
- Cyber- & IT-Security (M.Sc.)

Lehr- und Lernformen: Lab

- 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 mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativem Lernen

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.)
- Cyber- & IT-Security (M.Sc.)
- Data Science & Management (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs

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

Basisliteratur

- Literatur in Abhängigkeit von der gewählten Themenstellung

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

SCHWERPUNKT I: Informatik für Cyber- & IT-Security

SPI-1 Informatik für Cyber Security I

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 Python für die Netzwerkprogrammierung nutzen und für die Entwicklung von Netzwerk-Tools und -anwendungen verwenden.
- Sie kennen die grundlegenden Konzepte der Netzwerkprogrammierung, wie z.B. IP-Adressen, Ports, Protokolle
- Sie können Python-Module wie sockets, requests oder urllib verwenden.
- Sie kennen Techniken zur Implementierung von Client-Server-Anwendungen und können diese anwenden.
- Sie kennen Techniken zur Verwaltung von Netzwerkverbindungen und Übertragung von Daten und können diese anwenden.
- Sie kennen Techniken zur Fehlerbehandlung und Debugging in Netzwerkanwendungen und können diese anwenden.
- Sie kennen Techniken zur Sicherung von Netzwerkverbindungen und Datenübertragung und können diese anwenden.

Inhalte

- Verwendung von sockets zur Verbindung mit Netzwerkdiensten
- Implementierung von TCP und UDP Protokollen
- Verarbeitung von Netzwerknachrichten (Parsing, Serialisierung)
- Verwendung von verschiedenen Netzwerkbibliotheken wie twisted, asyncio, etc.
- Erstellung von Netzwerkanwendungen wie Server und Clients
- Verwendung von Protokollstapel-Modellen (OSI, TCP/IP)
- Debugging und Fehlerbehebung von Netzwerkproblemen
- Integrierung von Netzwerkfunktionalitäten in bestehende Anwendungen

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Matthes, E. Python Crash Course, 2nd Edition: A Hands-On, Project-Based Introduction to Programming (2019). No Starch Press
- Rhodes, B. Foundations of Python Network Programming (2014). Apress
- Jorgensen, B. Beej's Guide to Network Programming: Using Internet Sockets (2019). Independently published

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

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

SPI-2 Informatik für Cyber Security II

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 können Sicherheitsmaßnahmen für Computer- und Netzwerksysteme programmieren.
- Sie kennen die Grundlagen der Kryptographie und können Verschlüsselungsmethoden in der Programmierung anwenden.
- Sie kennen verschiedenen Arten von Sockets und deren Anwendungen.
- Sie können eigene Netzwerkprogramme entwickeln und debuggen.
- Sie kennen Sicherheitsproblemen im Zusammenhang mit Netzwerkprogrammierung und deren Lösungen.
- Sie können Netzwerksicherheitsmaßnahmen in eigene Programme implementieren.

Inhalte

- Verständnis der Grundlagen von Netzwerkprotokollen (TCP, UDP, IP, etc.)
- Erstellung von Netzwerkverbindungen mithilfe von Sockets
- Implementierung von Sicherheitsmaßnahmen wie Verschlüsselung und Authentifizierung
- Implementierung von Client-Server-Modellen
- Fehlerbehandlung und Timeout-Verfahren
- Multithreading und parallele Verarbeitung von Anfragen
- Verwendung von Frameworks und Bibliotheken zur Unterstützung der Netzwerkprogrammierung

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Fall, K., Stevens, W. TCP/IP Illustrated Volume 1: The Protocols (2011). Pearson
- Jorgensen, B. Beej's Guide to Network Programming: Using Internet Sockets (2019). Independently published
- Sarker, F. Python Network Programming Cookbook (2014). Packt Publishing

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

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.)
- Cyber- & IT-Security (M.Sc.)

Lehr- und Lernformen: Projekt

- 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
- 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 Sozialfor- schung. 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: Tools & Applications in Cyber- & IT-Security

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.
- Sie haben ein vertieftes Verständnis der Einsatzmöglichkeiten von Technologien im Rahmen der Prävention, Detektion und Abwehr. Sie können Einsatzchancen und Limitationen verstehen, erläutern und bewerten.
- Sie kennen verschiedene Technologien und Tools und können sie an- wenden, um eigene Sicherheitsanalysen vorzunehmen.
- Sie 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

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Die Studierenden haben ein erweitertes Verständnis der IT-Komponenten und Systeme für Cybersicherheit.
- Sie verstehen technologische Maßnahmen und können den kontinuierlichen Betrieb technologischer Lösungen für Cybersicherheit beschreiben.
- Sie 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.
- Sie 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

Keine

Verwendbarkeit

- Cyber- & IT-Security (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.)
- Cyber- & IT-Security (M.Sc.)

Lehr- und Lernformen: Projekt

- 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
- 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 Sozialfor- schung. 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: Cyber Security Management

SPIII-1 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.
- Sie sind in der Lage eigene Managementsysteme zu implementieren und zu betreiben.
- Sie können Synergieeffekte durch den Einsatz der unterschiedlichen Managementsysteme 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

- Cyber- & IT-Security (M.Sc.)
- Cybersecurity & Management (MBA)

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
- Projektarbeit in (virtuellen) Teams

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%

SPIII-2 Grundlagen von Audits, Reviews und Assessments

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 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

- Cyber- & IT-Security (M.Sc.)
- Cybersecurity & Management (MBA)

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%)

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.)
- Cyber- & IT-Security (M.Sc.)

Lehr- und Lernformen: Projekt

- 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
- 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 Sozialfor- schung. 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%)

WAHLPFLICHTMODULE (WP)

WP1 Systemsicherheit

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 grundlegenden Konzepte der Systemsicherheit, Verschlüsselung, Authentifizierung, Netzwerksicherheit und Bedrohungserkennung.
- Sie können sichere Systeme entwerfen und implementieren.
- Sie kennen relevante Tools und Technologien zur Überwachung und Verteidigung von Netzwerken und Systemen.
- Sie kennen Compliance-Anforderungen und deren Anwendung auf Systemsicherheitssysteme.
- Sie können sicherheitsrelevante Probleme identifizieren und mit zielgerichteten Maßnahmen reagieren.
- Sie kennen die rechtlichen Aspekte der Systemsicherheit, wie z.B. Datenschutzgesetze und -bestimmungen.
- Sie können Sicherheitsrichtlinien und -verfahren entwickeln und umsetzen.
- Sie haben ein umfassendes Verständnis von Angriffstechniken und -methoden und deren Abwehr.
- Sie können Notfallpläne für den Umgang mit Sicherheitsvorfällen entwickeln und umsetzen.
- Sie kennen die Rolle von Systemsicherheit in einem Unternehmen und im Geschäftsbetrieb.

Inhalte

- Grundlagen der Systemsicherheit
- Kryptographie und Verschlüsselungstechniken
- Netzwerksicherheit und Firewall-Technologien
- Analysieren und Verhindern von Angriffen auf IT-Systeme
- Sicherheit von Cloud-Computing und Internet of Things (IoT)
- Identitäts- und Zugriffsmanagement
- Compliance und Regulierungen
- Disaster Recovery und Business Continuity Management
- Ethik und Verantwortung im Bereich Systemsicherheit
- Praktische Anwendungen von Systemsicherheit durch Projektarbeiten und Fallstudien

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Horster, P. (Hrsg.) Systemsicherheit: Grundlagen, Konzepte, Realisierungen, Anwendungen (2012). DuD-Fachbeiträge
- Eckert, C. (2018). *IT-Sicherheit*. De Gruyter.
- 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%)

WP2 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 die Grundlagen von Cybersecurity in Operational Technology (OT).
- Sie kennen Methoden zur Identifizierung von Sicherheitsrisiken in OT-Systemen und Lösungen zur Absicherung von OT-Systemen vor Cyberangriffen.
- Sie verstehen die Zusammenhänge zwischen IT- und OT-Systemen im Hinblick auf Cybersecurity.
- Sie können Techniken zur Überwachung und Detektion von Cyberangriffen in OT-Systemen anwenden.
- Sie kennen die Anforderungen an die Cybersecurity in verschiedenen Branchen, Energieversorgung, Produktion, Verkehr.
- Sie können Methoden zur Durchführung von Penetrationstests in OT-Systemen auswählen und anwenden.
- Sie kennen Incident Response und Notfallmanagement im Kontext von Cyberangriffen in OT-Systemen.

Inhalte

- Einführung in die Konzepte der Cybersicherheit in operativen Technologien
- Sicherheitsrisiken und Bedrohungen in industriellen Steuerungssystemen (ICS/OT)
- Maßnahmen zur Vermeidung von Cyberangriffen auf ICS/OT-Systeme
- Methoden zur Erkennung und Reaktion auf Cyberangriffe in ICS/OT-Umgebungen
- Regulierung und Compliance im Bereich der Cybersicherheit in ICS/OT
- IT-Sicherheitstechnologien und -lösungen für ICS/OT-Systeme
- Praktische Anwendung von Sicherheitskonzepten und -technologien in ICS/OT-Systemen
- Fallstudien und Simulationen von Cyberangriffen auf ICS/OT-Systeme
- Ethische und rechtliche Aspekte der Cybersicherheit in ICS/OT-Systemen

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (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

- Macaulay, T., Singer, B. Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS (2016). Auerbach Publications
- Knapp, E., Langill, J. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2014). Syngress
- Cardwell, K. Defense and Deception: Confuse and Frustrate the Hackers (2020). Newman Springs Publishing, Inc.

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

WP3 Agiles Projektmanagement

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 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.
- Sie haben ein Grundverständnis von Agilität und damit zusammenhängenden Werten und Prinzipien. Sie verstehen, wie Agilität im Projektmanagement förderlich eingesetzt werden kann.
- Sie 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 anhand agiler und hybrider Ansätze

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Data Science & Management (M. Sc.)
- Cyber- & IT-Security (M.Sc.)
- Corporate Entrepreneurship & Innovation (MBA)

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, In-nova- tion 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%)

WP4 Public-Key-Infrastructure

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 grundlegenden Konzepte und Technologien der Public Key Infrastruktur (PKI).
- Sie wissen um verschiedene Arten von Zertifikaten und deren Anwendungen.
- Sie können PKI-Systeme planen, implementieren und verwalten.
- Sie kennen Sicherheitsaspekte von PKI-Systemen und der Methoden zur Vermeidung von Angriffen.
- Sie sind in der Lage PKI-Systemen in Unternehmensnetzwerke und -anwendungen zu integrieren.
- Sie verstehen rechtliche und regulativen Anforderungen an PKI-Systeme.
- Sie können Methoden und Techniken zur Überwachung und Wartung von PKI-Systemen anwenden.

Inhalte

- Grundlagen der Kryptographie
- Prinzipien der Public Key Infrastruktur (PKI)
- Verfahren zur Erstellung und Verwaltung von digitalen Zertifikaten
- Anwendungen der PKI in verschiedenen Bereichen, elektronische Signatur, sichere Kommunikation
- Standards und Protokolle im Zusammenhang mit PKI (z.B. X.509, SSL/TLS, S/MIME)
- Sicherheitsprobleme und Angriffsmöglichkeiten in PKI-Systemen
- Implementierung und Verwaltung von PKI-Systemen

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Cyber- & IT-Security (M.Sc.)

Lehr- und Lernformen: Lab

- 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 mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativem Lernen

Basisliteratur

- Vacca, J. Public Key Infrastructure: Building Trusted Applications and Web Services (2004). Auerbach Publications
- Nash, A., Brink, D., Duane, W., Joseph, C. Implementing & Managing E-Security (2001). McGraw Hill Professional
- Klöp, P. PKI und CA in Windows-Netzwerken (2017). Rheinwerk Computing

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