Modulhandbuch
Masterstudiengang (M.Sc.)
Cyber Security
Vollzeit / Teilzeit

Stand: März 2019

Inhalt

Glossar

BP	Betriebspraktikum
BS	Blockseminar
ECTS	European Credit Transfer System
BL	Blended Learning
GA	Gruppenarbeit
GBWL	Grundlagen der Betriebswirtschaftslehre
HA	Hausarbeit
KO	Kolloquium
KR	Kurzreferat
LN	Leistungsnachweis
LP	Leistungspunkt
LVA	Lehrveranstaltung
LVF	Lehrveranstaltungsform
MoP	Modulprüfung
mP	Mündliche Prüfungen
PA	Projektarbeit
PL	Praxisorientierte Lehrveranstaltungen
PR	Präsentation
PZ	Präsenzzeit
R	Referat
S	Seminar
SK	Sprachkurse
SoSe	Sommersemester
SP	Studium Plus
sP	Schriftliche Prüfungen
SPJ	Studienprojekt
SSt	Selbststudium
SWS	Semesterwochenstunden
UE	Übung
VL	Vorlesung
VWL	Volkswirtschaftslehre
WiSe	Wintersemester
WL	Workload

Einführende Informationen zum Studium an der HDBW

Zielsetzung	Studierenden sind in der Lage ein Thema konzeptionell umfassend und tiefgreifend zu behandeln und die daraus gewonnen theoretischen Erkenntnisse auf eine praktische Fragestellung anwenden zu können
Informations-möglichkeiten	Grundlegende Informationen über Studieninhalte, Studienaufbau, -ablauf, Bewerbung und Prüfungsangelegenheiten erhalten Studieninteressierte unter www.hdbw-hochschule.de. Die fachliche Studienberatung, insbesondere hinsichtlich Inhalte des Studiums und Wahlmöglichkeiten, wird von den Fachstudienberatern der jeweiligen Fachbereiche durchgeführt.
Studien- und Prüfungsordnung	Für einen erfolgreichen Studienverlauf ist die Kenntnis und Einhaltung der Regelungen der Prüfungsordnung zwingend erforderlich. Prüfungsordnungen stehen unter www.hdbw-hochschule.de zum Download zur Verfügung.
Vorlesungssprache	Die Vorlesungen können in Deutscher oder Englischer Sprache angeboten werden. Hierzu ist ein Sprachlevel B2 oder ein adäquater Nachweis durch den Studierenden zu erbringen.
Studienaufbau Module Lehrinhalte Lehrveranstaltungen	Der Studiengang im Vollzeitmodus ist auf eine Regelstudienzeit von 3 Fachsemestern, im Teilzeitmodus auf 5 Fachsemestern ausgelegt. Jedes Modul besteht aus einer oder mehreren Lehrveranstaltungen (LVA) (Vorlesung, Seminar, Übung, etc.). Diese umfassen Pflicht- und Wahlpflichtveranstaltungen. Detaillierte Beschreibungen der Modul- und Veranstaltungsinhalte finden sich im Modulhandbuch des jeweiligen Studiengangs.
Leistungspunkte / Workload	Der Masterstudiengang umfasst 90 ECTS Punkte. Für den mit jedem Modul verbundenen Arbeitsaufwand (Workload / WL) werden Leistungspunkte (LP) nach dem European Credit Transfer System (ECTS) vergeben. Generell gilt: 30 Stunden WL = 1 LP. Jedes Modul wird durch eine Modulprüfung (MoP) abgeschlossen, die aus studienbegleitenden Leistungsnachweisen besteht (LN). LN werden i.d.R. benotet. Eine Leistung gilt als bestanden, wenn sie mindestens mit der Note 4,0 bewertet wurde. Für das Abschlussmodul werden 20 LP vergeben (18 für die Masterthesis und 2 für die Verteidigung). Detaillierte Beschreibungen der pro Modul geforderten LN finden sich im Modulhandbuch des jeweiligen Studiengangs. Regelungen zu den Prüfungsformen finden sich in der Studien- und Prüfungsordnung des jeweiligen Studiengangs. Der Workload im Vollzeitstudium beträgt ca. 900 Stunden (30 ECTS pro Semester), im Teilzeitmodus ca. 600 Stunden (20 ECTS pro Semerster).
Vorlesungs- und Prüfungszeitraum	Der Vorlesungszeitraum umfasst 16 Wochen. Das Wintersemester (WiSe) beginnt i. d. R. Anfang Oktober. Das Sommersemester (SoSe) beginnt i. d. R. Mitte März. Der Prüfungszeitraum findet jeweils von der 16. bis 18. Vorlesungswoche statt (1. Prüfungstermin). Der Nachschreibetermin findet in der Regel in den jeweils letzten beiden Wochen der Semesterferien statt bzw. nach Ankündigung (2. Prüfungstermin).
Anrechnung von Studienzeiten und praktischen Tätigkeiten	Für die Anrechnung von Studienzeiten sowie praktischen Tätigkeiten ist der Prüfungsausschuss zuständig.
Prüfungen und Wiederholung von Prüfungen	Studierende werden automatisch zu den Prüfungen des jeweiligen Fachsemesters angemeldet. Abmeldungen sind die Studiengangsadministration zu richten.

Inhalt des Studiengangs

Der Masterstudiengang ist dem Profiltyp „anwendungsorientiert“ zugeordnet. Daher umfasst der Studiengang folgende Qualifikationsziele:

1. Die Studierenden kennen die unterschiedlichen System- und Netzwerkarchitekturen und können sie hinsichtlich ihrer Sicherheit und der Bedrohungspotentiale beurteilen.

2. Die Studierenden beherrschen die wesentlichen theoretischen Grundlagen aus dem Umfeld Verschlüsselung und deren praktischen Einsatz.

3. Die Studierenden kennen Methoden und Werkzeuge, mittels derer Angriffe auf die verschiedenen Systeme vorgenommen werden können.

4. Die Studierenden wenden Methoden und Werkzeuge zu Erkennung, Schutz und Abwehr von Angriffen auf verschiedenen Ebenen und Wegen an und kennen Vorgehensweisen zur Desaster Recovery.

5. Die Studierenden kennen die Bedeutung von Sicherheit im gesamten Lebenszyklus von Anwendungen und sind in der Lage, Cyber Security Anforderungen vom Entwurf bis End-of-Life umzusetzen.

6. Die Studierenden kennen die wesentlichen organisatorischen und rechtlichen Aspekte im nationalen und internationalen Kontext sowie die Anforderungen an Governance und Compliance, die im Umfeld Cyber Security relevant sind. Die Studierenden kennen neueste Ansätze z.B. aus der Künstlichen Intelligenz, und deren Anwendungsmöglichkeiten in der Cyber Security.

7. Die Studierenden haben ein anwendungsorientiertes Verständnis der aufgelisteten Aspekte und sind befähigt, diese als Mitarbeiter in verantwortender Position im Bereich Cyber Security technisch und organisatorisch selbständig umzusetzen.

Aufbau und Struktur des Studiengangs

Der Masterstudiengang Cyber Security umfasst 90 ECTS Punkte bei einem Gesamtarbeitsaufwand (WL) von 2700 Stunden.

Das Studium besteht aus einem Kernbereich für alle Studierende mit 55 ECTS sowie zwei Wahl-Schwerpunktbereichen „Technik" und „Organisation und Management" mit jeweils 15 ECTS. Die Lehrveranstaltungen sind sehr anwendungsorientiert. Alle Lehrveranstaltungen folgen in ihrem didaktischen Konzept einem klaren Muster:

1. In jeder Lehrveranstaltung werden zunächst die relevanten theoretisch-konzeptionellen Grundlagen des jeweiligen Faches auf Basis des jeweils aktuellen Standes aus Wissenschaft und Praxis vermittelt.

2. Anhand von praxisnahen Lehrveranstaltungskomponenten (z.B. Referenten aus der Praxis, Fallstudiendiskussion) wird ein anwendungsorientiertes Grundverständnis geschaffen.

3. Alle Lehrveranstaltungen sind interaktiv und beinhalten bewertete oder nicht bewertete Projektarbeitskomponenten unterschiedlichen Ausmaßes. Da dies die Philosophie des gesamten, anwendungsorientierten Masterprogramms und jeder Lehrveranstaltung ist, wurde bewusst auf eine explizite Trennung zwischen Vorlesungen und Übungen verzichtet.

4. Durch die Einbindung internationaler Lehrender wird sichergestellt, dass sich die globale Natur digitaler Technologien und Geschäftsmodelle auch in der Vermittlung der Lehrinhalte wiederfindet.

Masterthesis

Das Studium schließt mit einer Masterthesis ab, in deren Rahmen die Studierenden zeigen sollen, dass Sie in der Lage sind ein Thema konzeptionell umfassend und tiefgreifend zu behandeln und die daraus gewonnen theoretischen Erkenntnisse auf eine praktische Unternehmensfragestellung anwenden können. Daher besteht die Erstellung der Masterthesis aus den folgenden drei Komponenten:

1. Der selbständigen Erstellung einer Masterarbeit im Umfang von bis zu 80 Seiten.

2. Die Verteidigung und Präsentation der Ergebnisse der Masterarbeit mit einem Prüfungsgespräch, in dessen Rahmen die Inhalte der Masterarbeit auch in Verbindung zu sonstigen Inhalten des Studiums gesetzt werden. Die Dauer soll 10 Minuten nicht überschreiten. Die Gesamtdauer der Verteidigung darf 30 Minuten nicht überschreiten.

Einen Überblick über den Aufbau des Studiums in Vollzeit und Teilzeit geben die folgenden Abbildungen:

Master CyberSecurity Vollzeit					
1. Semester					
Grundlagen Cyber Security - Introduction to Cyber Security	Kryptographie - Cryptography	Computersysteme und Netzwerke - Systems and Networks	Systemanalyse und Härtung - System Auditing and Hardening	Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	Python und Go, Human Factors in CySe, Ethik, Soft Skills (Projektmanagement, Story Telling, Kommunikation)- Python and Go for Security, Human Factors in CySe, Ethics, Soft Skills
2. Semester					
Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	Seminar: aktuelle Themen der Cyber Security	Reifegradmodelle - Security Maturity	Security Governance and Compliance	Sicherheitsmanagement - Security Manangement
			Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics	System- und Netzwerksicherheit - System and Network Security	Methoden der Künstlichen Intelligenz (KI) - AI Methods
3. Semester					
Incident Management and Disaster Recovery	Requirements Engineering and Threat Modelling	Masterthesis			

Legende
Modul für alle Teilnehmer
Schwerpunktmodul Technik
Schwerpunktmodul Management
WPF

Abbildung 1 - Studium im Vollzeitmodell

Master CyberSecurity Teilzeit			
1. Semester			
Grundlagen Cyber Security - Introduction to Cyber Security	Kryptographie - Cryptography	Computersysteme und Netzwerke - Systems and Networks	Systemanalyse und Härtung - System Auditing and Hardening
2. Semester			
Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	Reifegradmodelle - Security Maturity	Security Governance and Compliance	Sicherheitsmanagement - Security Manangement
	Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics	System- und Netzwerksicherheit - System and Network Security	Methoden der Künstlichen Intelligenz (KI) - AI Methods
3. Semester			
Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	Incident Management and Disaster Recovery	Requirements Engineering and Threat Modelling	Python und Go, Human Factors in CySe, Ethik, Soft Skills (Projektmanagement, Story Telling, Kommunikation)- Python and Go for Security, Human Factors in CySe, Ethics, Soft Skills
4 Semester			
Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud....)	Seminar: aktuelle Themen der Cyber Security		
5. Semester			
Masterthesis			

Legende
Modul für alle Teilnehmer
Schwerpunktmodul Technik
Schwerpunktmodul Management
WPF

Abbildung 2 - Studium im Teilzeitmodell

Lehrveranstaltungsformen

Vorlesungen* (VL)
Vorlesungen dienen der Vermittlung theoretischer Kenntnisse, die meistens durch Übungen oder Laborunterricht ergänzt werden. Sie haben i.d.R. einen Semesterwochenstundenumfang von 2 Stunden. Zugehörige Skripte und Folien können für die Studierenden auf der entsprechenden Plattform online zur Verfügung gestellt werden. Vorlesungen schließen i.d.R. mit einer Prüfung ab. Die Art der Prüfung wird vom jeweiligen Fachdozenten festgelegt

Seminare* (S) und Blockseminare* (BS)
Seminare sind interaktive Lehrveranstaltungen, bei denen im Rahmen von kleinen Gruppen verschiedene Themen und Unterrichtsinhalte gemeinsam bearbeitet werden. Bestanteile der Zusammenarbeit sind zum Beispiel Übungen, Diskussionen und Referate. Seminare schließen entweder mit der Verschriftlichung eines Referates, dem Anfertigen einer Hausarbeit oder ein Klausur ab. Eine aktive Teilnahme wird für erfolgreiches Absolvieren der Veranstaltung vorausgesetzt. Blockseminare beinhalten dieselbe Lehrmethodik wie Seminare. Im Gegensatz zu normalen Seminaren umfassen Blockseminare jedoch i.d.R. ein jeweiliges Arbeitspensum von 8 Stunden und finden an festgelegten Tagen statt.

Übungen* (UE)
Übungen dienen hauptsächlich der Unterstützung von Vorlesungen. Je nach Modul können Sie auch ohne zugehörige Vorlesung angeboten werden. Im Rahmen der Übung werden theoretische Kenntnisse durch Übungsaufgaben wiederholt und gefestigt. Sie finden i.d.R. in Präsenzform statt und haben einen Semesterwochenstundenumfang von bis zu 2 Stunden, können aber auch in Form von Blended Learning angeboten werden. Für ein erfolgreiches Absolvieren der Veranstaltung wird eine aktive Teilnahme vorausgesetzt.

Sprachkurse* (SK)
Sprachkurse sind wie der Name bereits sagt, ausschließlich auf den Erwerb einer Fremdsprache ausgerichtet. Die Unterrichtsform gleicht der von Seminaren und zeichnet sich insbesondere durch interaktive Lehrmethoden aus. Leistungsnachweise werden zum Beispiel häufig in der Form von Referaten oder Präsentationen erbracht. Sprachkurse können zudem ebenso als Blockveranstaltung stattfinden. Auch bei ihnen gilt: eine aktive Teilnahme ist Voraussetzung für das Bestehen des Moduls ratsam.

Praxisorientierte Lehrveranstaltungen* (PL)
Praxisorientierte Lehrveranstaltungen dienen dem Erwerb von fachspezifischem Anwendungswissen und Schlüsselqualifikationen. In der Regel umfassen sie dieselben Lehrmethoden wie Seminare und Übungen. Darüber hinaus können sie in Form von Exkursionen, Workshops und Trainings stattfinden.

Alle mit * gekennzeichneten Lehrveranstaltungsformen werden im didaktischen Konzept des Blended Learnings (BL) angeboten. Blended-Learning-Veranstaltungen dienen der Darstellung und Bearbeitung größerer Stoffgebiete, weshalb sie ebenso als Teil von Vorlesungen und häufig als Ergänzung von Übungen stattfinden. Sie dienen aber auch der

Vertiefung theoretischer Inhalte mit Fallbeispielen und Übungsaufgaben. Blended-Learning-Veranstaltungen umfassen sämtliche Lehrmethoden sowohl in Form von Präsenz- als auch virtueller Veranstaltung. Über das Lernmanagementsystem (LMS) können den Teilnehmern verschiedene Lernunterlagen wie Scripts und Tutorials sowie Audios und Videos zur Verfügung gestellt werden. Die detaillierte Beschreibung des Unterrichtsverlaufs sowie die Termine für die Präsenzveranstaltungen werden zu Beginn des jeweiligen Semesters im LMS und bei der zuständigen Fachstudienberatung zur Verfügung gestellt. Während des gesamten laufenden Semesters stehen die Tutoren bei inhaltlichen sowie organisatorischen Fragen zur Verfügung.

Studienprojekt (SPJ)
Studienprojekte sind Lehrveranstaltungen mit erhöhtem Arbeitsaufwand. Sie werden zum Beispiel im Rahmen eines Forschungsprojektes oder einer Gruppenarbeit durchgeführt und fördern insbesondere die selbständige Anwendung forschungstypischer Arbeitsweisen, weshalb sie nicht selten auch der Themenfindung von Abschlussarbeiten dienen. Studienprojekte werden im Sinne des Selbststudiums umgesetzt und setzten daher i.d.R. keine festen Präsenzzeiten voraus.

Selbststudium (SSt)
Das Selbststudium dient der selbstständigen Vor- und Nachbereitung von LVA und wird für alle Module vorausgesetzt.

Kolloquium (KO)
Kolloquien umfassen i.d.R. interaktive Diskussionsrunden innerhalb derer Themen referiert und präsentiert werden. Sie finden immer als Präsenzveranstaltung statt. Häufig dienen sie während des Studienabschluss der Unterstützung bei der Erstellung der Bachelorarbeit.

Lernmanagementsystem (LMS)
Das Lernmanagementsystem (LMS) ist ein elektronisches, webbasiertes System, das Kursinhalte in strukturierter Form auf einer Plattform darstellt und Lehrenden wie auch Teilnehmenden interaktive Funktionen für das kollaborative Arbeiten zur Verfügung stellt. Es umfasst die Teilnehmerverwaltung, das Dokumentenmanagement, Leistungsmessungsfunktionen, Kalenderfunktionen und die Möglichkeit zur Einbindung von interaktiven Lerneinheiten. Weitere Informationen zum LMS sind bei der Studienberatung des jeweiligen Fachbereichs zu erhalten.

Leistungsnachweise

Modulprüfung (MoP)
Jedes Modul kann aus einer oder mehreren Lehrveranstaltungen (LVA) zusammengesetzt sein. Pro Modul findet eine Modulprüfung (MoP) statt, die die Bestandteile einer oder mehrerer LVA umfassen kann. Die MoP kann aus unterschiedlichen Leistungsnachweisen (LN) bestehen. Diese können veranstaltungsbegleitender Natur sein oder im Prüfungszeitraum am Ende des Semesters erbracht werden. Die Modulnote errechnet sich aus der in der MoP erreichten Leistung gemäß dem zu Beginn des Moduls bekannt gegebenen Schemas. Folgende Prüfungsformen können im Rahmen der MoP als LN vorkommen (die vorgeschriebene Prüfungsform findet sich jeweils bei den entsprechenden Modulen im Handbuch):

Schriftliche Prüfungen (sP)
Schriftliche Prüfungen haben i.d.R. einen Umfang von 60 Minuten und finden am Ende des Semesters statt. Sie werden meistens von den Leitern oder Leiterinnen der entsprechenden Lehrveranstaltungen gestellt und bewertet. Bei Klausuren ist generell der Studierendenausweis inklusive eines amtlichen Ausweises mit Lichtbild mit sich zu führen.

Mündliche Prüfungen (mP)
Mündliche Prüfungen finden entweder im Einzelgespräch oder in Form von Gruppen statt. Je nach Bedeutung der Prüfung umfassen sie einen Zeitraum von mindestens 15 und maximal 60 Minuten. Meistens finden sie gegen Ende des Semesters statt.

Hausarbeit (HA)
Hausarbeiten sind schriftliche Ausarbeitungen eines mit dem zuständigen Professor abgestimmten Themas. Ihr Umfang kann zwischen 5 und 25 DIN-A 4 Seiten betragen. Die Bearbeitungszeit für Hausarbeiten beträgt höchstens vier Wochen. Sie können meistens in der vorlesungsfreien Zeit bearbeitet werden, wobei es zu empfehlen ist sie bereits im Laufe des Semesters fertig zu stellen, um den Prüfungsstress am Ende des Semesters zu reduzieren.

Referat (R)
Referate sind eine mündliche Prüfungsleistung in der ein zuvor mit dem zuständigen Lehrenden oder der zuständigen Lehrenden abgesprochenes Thema vor den Kommilitonen der Lehrveranstaltung präsentiert wird. Die Inhalte sollten wissenschaftlich recherchiert sein. Alle Thesen des Referats sollten auf einem Thesenballt für die Mitstudierenden zusammengefasst werden. Die Dauer eines Referats umfasst zwischen 20 und 45 Minuten, je nach Absprache mit dem zuständigen Lehrenden oder der zuständigen Lehrenden. Referate können auch in Gruppen vorbereitet und gehalten werden. Ergänzt wird es in der Regel durch eine schriftliche Ausarbeitung in Form einer Hausarbeit.

Kurzreferat (KR)
Kurzreferate unterscheiden sich von Referaten lediglich im Hinblick auf ihre Länge: sie umfassen höchstens 10 Minuten. Alle anderen Aspekte sind gleich.

Präsentation (PR)
Präsentationen können entweder als Einzelleistung oder in Form einer Gruppenarbeit durchgeführt werden. Die Arbeitsergebnisse werden vor den Mitstudierenden und dem Leiter bzw. der Leiterin der entsprechenden Lehrveranstaltung präsentiert. Im Gegensatz zum Referat ist die Präsentation umfangreicher in Inhalt, Methodik und Darstellung.

Projektarbeit (PA)
Projektarbeiten können als Hausarbeit oder als Präsentation angefertigt werden. Das Thema der Projektarbeit wird zuvor mit dem zuständigen Lehrenden oder der zuständigen Lehrenden festgelegt. Projektarbeiten können entweder als Einzelleistung oder in Form einer Gruppenarbeit durchgeführt werden.

Die Form der Prüfung wird am Anfang des Semesters durch den verantwortlichen Dozenten des Modules festgelegt und auf einem den Studenten zugänglichen Informationssystem der HDBW mitgeteilt.

Weitere Details zu Prüfungsarten, Dauer und Bedingungen finden sich die jeweils aktuellen Studienprüfungsordnung (SPO) des Studiengangs bzw. der Allgemeinen Prüfungsordnung (APO) der Hochschule.

Literatur

Der Dozent, die Dozentin der jeweiligen Lehrveranstaltung legt vor Beginn des Semesters fest, welche begleitende Literatur benötigt wird. Diese Information wird zur Beginn der Veranstaltung bzw. über das LMS bekannt gegeben. Weitere unterstützende Materialien (z. B. Skripte, Übungsaufgaben, Vorlesungsfolien, etc.) werden über das LMS sowie vorliegenden Handapparat rechtzeitig zur Verfügung gestellt.

Modulübersicht

MoNr.	Module mit Lehrveranstaltungen	LVF	V	SWS	MoP	LP*	Sem VZ	Sem TZ
CSM1	**Grundlagen Cyber Security - Introduction to Cyber Security**				**sP**	**5**	**1**	**1**
CSM1	Grundlagen Cyber Security - Introduction to Cyber Security	VL/UE	P	4				
CSM2	**Kryptographie - Cryptography**				**sP**	**5**	**1**	**1**
CSM2	Kryptographie - Cryptography	VL/UE	P	4				
CSM3	**Computersysteme und Netzwerke - Systems and Networks**				**sP**	**5**	**1**	**1**
CSM3	Computersysteme und Netzwerke - Systems and Networks	VL/UE	P	4				
CSM4	**Systemanalyse und Härtung - System Auditing and Hardening**				**PA**	**5**	**1**	**1**
CSM4	Systemanalyse und Härtung - System Auditing and Hardening	VL/UE	P	4				
CSM5	**Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle**				**sP**	**5**	**1**	**3**
CSM5	Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	VL/UE	P	4				
CSM6	**Wahlpflichtmodul**					**5**	**1**	**3**
CSM6-1	Python und Go – Python and Go	VL/UE	WP	2	**PA**	**2,5**	**1**	**3**
CSM6-2	Human Factors in Cyber Security	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**
CSM6-3	Ethik – Ethics	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**
CSM6-4	Softskills – Softskills	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**
CSM7	**Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,…) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)**				**PA**	**5**	**2**	**4**
CSM7	Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,…) - Security Aspects in	PA	P	4				

	Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)							
CSM8	**Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy**				**sP**	**5**	**2**	**2**
CSM8	Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	VL/UE	P	4				
CSM9	**Seminar: aktuelle Themen der Cyber Security**				**PA**	**5**	**2**	**4**
CSM9	Seminar: aktuelle Themen der Cyber Security	VL/UE	P	4				
Wahlpflichtbereich Technik								
CSMT1	**Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics**				**PA**	**5**	**2**	**2**
CSMT1	Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics	VL/UE	P	2				
CSMT2	**System- und Netzwerksicherheit - System and Network Security**				**PA**	**5**	**2**	**2**
CSMT2	System- und Netzwerksicherheit - System and Network Security	VL/UE	P	4				
CSMT3	**Methoden der Künstlichen Intelligenz (KI)**				**sP**	**5**	**2**	**2**
CSMT3	Methoden der Künstlichen Intelligenz (KI)	VL/UE	P	4				
Wahlpflichtbereich Organisation und Management								
CSMO1	**Reifegradmodelle - Security Maturity**				**sP**	**5**	**2**	**2**
CSMO1	Reifegradmodelle - Security Maturity	VL/UE	P	2				
CSMO2	**Security Governance and Compliance**				**sP**	**5**	**2**	**2**
CSMO2	Security Governance and Compliance	VL/UE	P	4				

CSMO3	**Sicherheitsmanagement - Security Manangement**				**sP**	**5**	**2**	**2**
CSMO3	Sicherheitsmanagement - Security Manangement	VL/UE	WP	4				
CSM10	**Incident Management and Desaster Recovery**				**PA**	**5**	**3**	**3**
CSM10	Incident Management and Desaster Recovery	VL/UE	WP	4				
CSM11	**Requirements Engineering and Threat Modelling**				**sP**	**5**	**3**	**3**
CSM11	Requirements Engineering and Threat Modelling	VL/UE	WP	4				
CSMMT	**Master-Thesis**						**3**	**5**
CSMMT1	Masterthesis	SSt	P		**HA**	**18**		
CSMMT2	Verteidigung / defense	mP	P		**mP**	**2**		

Modulbeschreibungen

Grundlagen Cyber Security - Introduction to Cyber Security	
Modulnummer	**CSM1**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Prof. Dr. Sabine Rathmayer, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Studierende erhalten einen Einblick in die verschiedenen Aspekte der Cyber Sicherheit und werden in der Lage versetzt, die Bedeutung und Zusammenhänge verschiedener technischer und organisatorischer Einflussfaktoren auf die Cyber Sicherheit zu verstehen. Mit den erworbenen Kenntnissen können die Studierenden systematische Bewertungen des Schutzbedarfs und des Sicherheitsniveaus - moderner IT-Systeme, - IT-Infrastrukturen sowie - OT (Operational Technology) vornehmen, in die auch in der Praxis häufig noch unterschätzte nicht-technische Faktoren einfließen. Hierbei wird insbesondere nach kleinen, mittleren und großen Unternehmen differenziert. Darüber hinaus spielt vor allem auch das Verständnis für die verschiedenen Akteursgruppen und deren Motivation eine wichtige Rolle.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: Klassische Methoden der technischen und organisatorischen Informationssicherheit, u.a. - Bedrohungen und Gefährdungen, Risikoanalysen - BSI IT-Grundschutz - Grundlagen der angewandten Kryptographie - Security Engineering - Sicherheitsmodelle und -mechanismen und deren Umsetzung in verteilten Systemen und Rechnernetzen - Sicherheit mobiler Endgeräte - praktische Aspekte der Informationssicherheit - Security Incident Response mit Breach- und Malware-Analyse - Social Engineering: Faktor Mensch in der Informationssicherheit aus Angreiferperspektive - Identity & Access Management, Datenschutz und Privacy - Sicherheit ausgelagerter Dienste (z.B. im Cloud Computing)
Literatur	- Whitman, M.; Mattord, H.: Principles of Information Security, 5th Edition, Cengage Learning, Boston 2016 - Graham, J.; Howard, R.; Olson, R.: Cyber Security Essentials, CRC Press, Boca Raton 2011 - Voeller, J.: Cyber Security, Wiley 2014

Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	Digitale Technologie (MA)
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Kryptographie - Cryptography	
Modulnummer	**CSM2**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Dr. Stephan Spitz , weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Die Studierenden lernen in dieser Einführung die Grundlagen der Verschlüsselungsmethodik und der modernen Kryptographie kennen. Sie lernen Industriestandards und deren Umsetzung verstehen. Das Modul beinhaltet moderne Kryptographie über Algorithmen und Kryptosysteme, Kryptoanalyse und Best Practices für die Anwendung sowie Implementierung in Softwaresystemen. Zudem werden die Grundzüge der Quantenkryptographie vermittelt.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Klassische Kryptographie: Substitution, Transposition, Rotor Machine - Moderne Kryptographie: Strom- und Blockverschlüsselung, DES, AES - Hash und Datenintegrität: SHA - Asymmetrische Kryptographie: Diffie-Hellman, RSA, Elliptische Kurve - Public Key Infrastruktur: X.509-Zertifikate, Keymanagement, Kerberos, SSH, SSL/TLS
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Spitz, S., Pramateftakis, M., Swoboda, J.: Kryptographie und IT-Sicherheit, Vieweg+Teubner Verlag 2011 - Schmeh, K.: Kryptografie, 6. Auflagedpunkt, Heidelberg 2016 - Stallings, W.: Cryptography and Network Security, 7th Edition, Pearson, Essex 2017 - Schneier, B.: Applied Cryptography, Wiley, Indianapolis 1996
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Computersysteme und Netzwerke - Systems and Networks	
Modulnummer	**CSM3**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Prof. Dr. Jianmin Chen, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Das Modul vermittelt die Prinzipien und Techniken, die in Betriebssystemen und Kommunikationsnetzen, insbesondere in der TCP/IP-Protokollsuite verwendet werden. Zu den Themen gehören zudem drahtlose und zelluläre Protokolle sowie RFID und andere WPAN (Wireless Personal Area Network). Darüber hinaus wird ein Überblick über Technologien und Spezifika bei „Operational Technology“ gegeben.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Rechnerarchitektur und Betriebssysteme - Netzwerkarchitekturen und Kommunikationsprotokolle - Netzwerkschichten und OSI-Referenzmodell - Local Area Network - Internet und Intranet - Virtual Private Network - Mobile Netzwerke und WLAN - WPAN und RFID - Operational Technology (OT) und Supervisory Control and Data Acquisition (SCADA)
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Bryant, R.; O'Hallaron, D.R.: Computer systems, Boston, Pearson 2011 - Tanenbaum, A.: Computernetzwerke, International Edition 2011 - Tanenbaum, A.: Modern Operating Systems, 4. Edition, Boston, Pearson 2015
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Systemanalyse und Härtung - System Auditing and Hardening	
Modulnummer	**CSM4**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Dr. Max Moser, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Die Studierenden kennen exemplarisch Cyber Attacken mittels derer Schwachstellen in Netzwerken, Betriebssystemen und Anwendungen gefunden werden können. Die Praxis erfolgt anhand verschiedener Techniken und aktuell verfügbarer Werkzeuge. Es werden Passwörter und drahtlose Netzwerke gehackt sowie Webapplikationen auf Schwachstellen untersucht. Anhand von Frameworks (Metasploit, w3af, ...) werden Exploits getestet und eigene Module geschrieben. Weitere Lernziele sind das Automatisieren von Social Media Attacken, das Umgehen von Antiviren Software und die Einnahme von kompletten Rechnern. Die Studierenden kennen Ansätze und Methoden zur Abwehr und Härtung der untersuchten Angriffsszenarien.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - IT-Sicherheit und Sicherheitsmaßnahmen - Motivation und Schwachstellen von vernetzten Rechnersystemen - Verfahren, Mechanismen und Tools zur Systemanalyse - Verfahren, Mechanismen und Tools zur Systemhärtung - Intrusion Detection und Prevention-Systeme zur Angriffserkennung und -abwehr - Logfileanalyse und Analyse von Webaktivitäten - Kali LInux, Wireshark, Nmap and Burp Suite
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Donald A. Tevault: Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats, Packt Publishing - Eric D. Knapp, Joell T. Langill: Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Syngress Press
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	
Modulnummer	**CSM5**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Dagmar Moser, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Die Studierenden kennen die Bedeutung von Sicherheit in der Anwendungsentwicklung. Während lange Zeit bei Security der Schwerpunkt auf der Absicherung von Systemen und Netzwerken lag, rückten in den letzten Jahren die Applikationen selbst verstärkt in den Fokus. Durch die frühzeitige Berücksichtigung von Sicherheit in der Applikationsentwicklung kann nicht nur das Sicherheitsniveau erheblich verbessert werden, sondern auch Aufwand und Komplexität in anderen Bereichen reduziert werden. Über das reine "Coding" deutlich hinaus wird der gesamte Lebenszyklus der Applikationen - von der Anforderungsanalyse bis hin zum Deployment und der Reaktion auf sicherheitsrelevante Ereignisse - betrachtet. Unabhängig vom gewählten Software-Entwicklungsprozess (V-Modell, RUP, SCRUM, etc.) werden Security Aspekte in jeder Entwicklungsphase, in jeder Iteration und in jedem Sprint bewusst eingeplant und umgesetzt. Die Studierenden kennen die Erhebung von Sicherheitsanforderungen, die Identifizierung und Bewertung von Sicherheitsrisiken und die Planung konkreter Maßnahmen. In der Entwurfs- und Implementierungsphase kommen bekannte Architektur-Prinzipien und Design Patterns, sowie Grundregeln für die sichere Codierung zum Einsatz. Insbesondere bei einem iterativen oder agilen Vorgehen begleiten Tests den kompletten Entwicklungsprozess. Auch hier werden Sicherheitstests von systematisch integriert. Exemplarisch werden hierbei etablierte Methoden aus der Praxis vorgestellt.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Sicherheitsanforderungen - Sicherer Software-Entwurf, u.a. Secure Design Principles und Secure Design Patterns - Sicheres Codieren - Sicherheitstests, u.a. Penetration Testing, Grey-Box - Build und Deployment - Beispiele etablierter Modelle
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Basiswissen Sichere Software, Sachar Paulus, dpunkt-Verlag - Microsoft Security Development Lifecycle https://www.microsoft.com/en-us/sdl - Security Engineering, Ross Anderson, Wiley Verlag

	- Secure by Design, Dan Bergh Johnsson, Daniel Deogun, Daniel Sawano, Manning-Verlag - Securing DevOps - Security in the Cloud, Julien Vehent, Manning-Verlag
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Python und Go – Python and Go	
Modulnummer	**CSM6-1**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Dr. Max Moser, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	2 SWS: PL
Arbeitsaufwand (WL)	75h: 30h BL / 45h SSt
LP (ECTS)	2,5
MoP / LN	PA
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Die Studierenden lernen in diesem Modul zwei der der gebräuchlichsten Programmiersprachen im Kontext sicherheitsrelevanter Entwicklungen kennen: Python und Go. Über beide sind eine schnelle Entwicklung sowohl von einfachen Tools als auch von komplexen Anwendungen möglich. Darüber hinaus ermöglicht Go die Erstellung eigenständiger Programme ohne Abhängigkeiten und vereinfacht so die Installation und Nutzung. Auch wenn für den offensiven und defensiven Einsatz in der Cybersicherheit bereits verschiedene Tools zur Verfügung stehen, die in der Regel grafische Benutzeroberflächen anbieten oder über die Kommandozeile bedient werden können, z.B. Metasploit, gibt es viele Situationen, in denen individuellere Aktionen erforderlich sind oder in denen bestehende Tools kombiniert oder integriert werden müssen. Die Fähigkeit, Logik schnell für kundenspezifische Zwecke zu implementieren, kann sich als eine entscheidende Kompetenz erweisen.
Verbindlichkeit	Wahlpflicht, zwei aus den angebotenen Modulen
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Geschichte und wesentliche Paradigmen von Python und Go - Einrichtung der Entwicklungsumgebung zur Implementierung von "Hello World". - Einführung in die wichtigsten Sprachkonstrukte und -funktionen - Nutzung der bestehenden Standardbibliotheken - Verwendung von spezialisierten Bibliotheken - Anwendungen von Python und Go in "Red Team" und "Blue Team" Situationen - z.B. Reverse-Tunneling - z.B. Netzwerkanalyse
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - "Python Crash Course - A Hands-On, Project-Based Introduction to Programming" by Eric Matthes, NoStarch Press - "Black Hat Python - Python Programming for Hackers and Pentesters" by Justin Seitz, NoStarch Press - "Gray Hat Python - Python Programming for Hackers and Reverse Engineers" by Justin Seitz, NoStarch Press - "Introducing Go" by Caleb Doxsey, O-Reilly - "A Tour to Go", https://tour.golang.org

	- "Go by Example", https://gobyexample.com/ - "Black Hat Go - Go Programming for Hackers and Pentesters" by Tom Steele, Chris Patten, and Dan Kottmann, NoStarch Press
Sonstige Informationen	Gruppenarbeit
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Human Factors in Cyber Security	
Modulnummer	**CSM6-2**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Prof. Dr. Sabine Rathmayer, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	2 SWS: PL
Arbeitsaufwand (WL)	75h: 30h BL / 45h SSt
LP (ECTS)	2,5
MoP / LN	PR
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Die Studierenden kennen die Bedeutung des Faktors Mensch im Bereich der Cyber Securiy. Sie entwickeln ein Verständnis für die Zusammenhänge zwischen Informationssicherheit, Privatsphäre und Benutzbarkeit von Informationssystemen. Die Studierenden wissen, welche Risiken durch den Menschen als Schwachstelle und als Betroffenen entstehen und welche Lösungsansätze möglich sind.
Verbindlichkeit	Wahlpflicht, zwei aus den angebotenen Modulen
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Überblick über unterschiedlichen Aspekte des Faktors Mensch in der Cyber Security - Recherche, Präsentation und Diskussion unterschiedlicher Aspekte und Herausforderungen
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Usable Security: History, Themes, and Challenges (Synthesis Lectures on Information Security, Privacy, and Trust): Simson Garfinkel und Heather Richter Lipford. 2014 - Melanie Volkamer, Karen Renaud: Mental Models - General Introduction and Review of Their Application to Human-Centred Security. In Number Theory and Cryptography (2013): 255-280: https://link.springer.com/chapter/10.1007/978-3-642-42001-6_18 - Melanie Volkamer, Karen Renaud: Mental Models - General Introduction and Review of Their Application to Human-Centred Security. In Number Theory and Cryptography (2013): 255-280: https://link.springer.com/chapter/10.1007/978-3-642-42001-6_18 - Melanie Volkamer, Karen Renaud: Mental Models - General Introduction and Review of Their Application to Human-Centred Security. In Number Theory and Cryptography (2013): 255-280: https://link.springer.com/chapter/10.1007/978-3-642-42001-6_18 -
Sonstige Informationen	Gruppenarbeit nach Einführungspräsentation
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene

	arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Ethik - Ethics	
Modulnummer	**CSM6-3**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Dr. Josephine Müller, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	2 SWS: PL
Arbeitsaufwand (WL)	75h: 30h BL / 45h SSt
LP (ECTS)	2,5
MoP / LN	PR
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Die Studierenden kennen die Bedeutung der Diskussion über Ethik im Zusammenhang mit Cyber Security. Die Durchsetzung der Cybersicherheit birgt die Gefahr, dass andere grundlegende Werte wie Gleichheit, Fairness oder Privatsphäre übergangen werden. Gleichzeitg kann das Herunterspielen der Cybersicherheit das Vertrauen der Bürger in die digitale Infrastruktur massiv beeinträchtigen.
Verbindlichkeit	Wahlpflicht, zwei aus den angebotenen Modulen
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Definition von Ethik insbesondere im Zusammenhang mit Cyber Security - Recherche, Präsentation und Diskussion unterschiedlicher Aspekte und Herausforderungen
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** Yaghmaei, Emad and van de Poel, Ibo and Christen, Markus and Gordijn, Bert and Kleine, Nadine and Loi, Michele and Morgan, Gwenyth and Weber, Karsten, Canvas White Paper 1 – Cybersecurity and Ethics (October 4, 2017). Available at SSRN: https://ssrn.com/abstract=3091909 or http://dx.doi.org/10.2139/ssrn.3091909
Sonstige Informationen	Gruppenarbeit nach Einführungspräsentation
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Softskills	
Modulnummer	**CSM6-4**
Dauer	1 Semester
Modulverantwortlicher	Silke Biermann
Dozent/en	Silke Biermann, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	2 SWS: PL
Arbeitsaufwand (WL)	75h: 30h BL / 45h SSt
LP (ECTS)	2,5
MoP / LN	PR
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Die Studierenden verfügen über umfassende Kenntnisse in den Bereichen Kommunikation, Präsentation und Moderation und entwickeln eine tiefere Sozialkompetenz. Die Studierenden sind in der Lage, verschiedene Moderations- und Präsentationstechniken im Vortrag, Interview und Trendforum anzuwenden.
Verbindlichkeit	Wahlpflicht, zwei aus den angebotenen Modulen
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Einführung in die grundlegenden Fragestellungen der Kommunikation, Präsentation und Moderation - Grundlagen über Kommunikationsprozesse, Unternehmenskommunikation, Präsentations- und Moderationsmethoden
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Watzlawick, P./Beavin J. H./ Jackson D. D. (2003): Menschliche Kommunikation; Formen, Störungen, Paradoxien. Bern. - Will, H. (2000): Mini Handbuch; Vortrag und Präsentation. Weinheim; Basel.
Sonstige Informationen	Gruppenarbeit
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,…) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	
Modulnummer	**CSM7**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Dr. Stephan Spitz, , weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1, CSM2, CSM3
Lernergebnisse des Moduls	Die Studierenden kennen spezifische Aspekte der Cybersicherheit aus verschiedenen Anwendungsbereichen. IoT auf Basis eingebetteter Systeme unter Kostendruck, offen zugängliche Umgebung und eingeschränkte Ressourcen stellen besondere Sicherheitsherausforderungen dar. Die industrielle Internet- und Betriebstechnologie mit einer großen installierten Basis von SCADA (Supervisory Control and Data Acquisition) wird zu einem wertvollen Ziel für Cyberangriffe. Das aufkommende Mobile- und Cloud Computing bringt mit seiner breiten Marktakzeptanz neue Herausforderungen für die Cybersicherheit mit sich.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: IoT systems and networks - Security and privacy principles of complex interconnected IoT - Types of threads, attacks and countermeasures - Confidentiality, authentication, integrity and availability OT (Operation Technology) / SCADA: - Threats and Vulnerabilities - Resilient Systems and Defence in Depth Cloud Computing: - Service models, key concepts and enabling technologies of cloud Computing - Confidentiality, availability and integrity - Risk management and division of responsibility - Trusted cloud Security Mobile Computing: - Threads and vulnerability of mobile smart devices - Security aspects of mobile network
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Colbert, E. (ed.): Cyber-security of SCADA and Other Industrial Control Systems, Springer 2016 - Loukas, G.: Cyber-Physical Attacks, Elsevier 2015 - Winkler, V.: Securing the Cloud, Elsevier 2011 - Industrial Internet Consortium: Industrial Internet of Things, Volume

	G4: Security Framework, 2016 - Vacca, J..: Cloud Computing Security, Taylor & Francis 2017
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	
Modulnummer	**CSM8**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Michaela Braun, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1, CSM2
Lernergebnisse des Moduls	Die Studierenden kennen die rechtlichen Aspekte von "Cyber-Security" insbesondere die regulatorischen Anforderungen der IT-Sicherheit und des Datenschutzes. Mit der globalen Vernetzung in einer flachen Welt, werden die gesetzlichen und regulatorischen Rahmen in Deutschland, EU, USA und anderen wichtigen Regionen mit ihren spezifischen Ausprägungen und Bedeutungen hinsichtlich Cyber Security behandelt. Dabei werden auch zahlreiche andere Rechtsgebiete, die betroffen sind, wie etwa das Gesellschaftsrecht (Best Practices der Unternehmensorganisation und Sorgfaltspflichten der Geschäftsleitung), das Versicherungsrecht, das Arbeitsrecht, aber auch die Transaktions- und Aufsichtspraxis thematisiert. Die Anforderungen aus diesen rechtlichen und regulatorischen Rahmen für die Compliance und Governance werden dargestellt. Darüber hinaus werden die dynamische Entwicklung der politischen und soziologischen Aspekte hinsichtlich Cyber Security, die als zukünftige Anforderungen in rechtliche, regulatorische über Interessengruppe normativ werden können, behandelt. Um den praktischen Nutzen zu erhöhen, wird dabei in der Regel zwischen den rechtlichen Anforderungen an eine Vorbeugung ("Preparedness") und den rechtlichen Leitplanken im Ernstfall ("Response") unterschieden.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Betrachtunger verschiedener Rechtsgebiete wie Gesellschaftsrecht, Versicherungsrecht, Arbeitsrecht, Strafrecht in Zusammenhang mit Cyber Security - Regulatorische Anforderungen - Regionale, nationale und internationale Aspekte - Maßnahmen zur Vorbeugung und im Ernstfall
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Gabel / Heinrich / Kiefner Rechtshandbuch Cyber-Security - Stallings, W. et al: Foundations of Modern Networking, Pearson 2016 - Kizza, J.: Computer Network Security and Cyber Ethics, 4th Edition. McFarland, Jefferson 2014
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.

Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Seminar: aktuelle Themen der Cyber Security	
Modulnummer	**CSM9**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Prof. Dr. Sabine Rathmayer, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1
Lernergebnisse des Moduls	Ausgewählte Themen werden anhand aktueller Veröffentlichungen aufgearbeitet. Die Themen werden jeweils zu Beginn des Semesters festgelegt. Die Abgabeformen sind Ausarbeitung und Vortrag. Hierbei werden die Studierenden in die wissenschaftliche Arbeit hinsichtlich Inhalt, Konzept, Durchführung und formalen Anforderungen eingeführt.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Recherche über aktuelle Themen und Entwicklungen aus dem Gebiet der Cyber Security - Aufbereitung und Präsentation der Recherche-Ergebnisse
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Aktuelle Literatur entsprechend der jeweiligen Themen
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen. Die Projektarbeit beinhaltet eine Präsentation.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Intrusion Detection + Digitale Forensik – Intrusion Detection +Digital Forensics	
Modulnummer	**CSMT1**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Dr. Max Moser,, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1, CSM4
Lernergebnisse des Moduls	In diesem Modul werden die Bausteine und Anforderungen an Intrusion Detection Systeme untersucht, die verschiedenen Ansätze untersucht und bewertet und praktische Einsätze eines IDS sowie ausgewählte IDS-Produkte betrachtet. Intrusion Detection Systeme, abgekürzt IDS, haben zum Ziel, auf Computer oder Netzwerke gerichtete Angriffe zu erkennen und sie zu melden. Damit ergänzen sie die Funktionen, die durch Firewalls üblicherweise gegeben sind, indem sie zusätzlich die Abläufe hinter der Firewall betrachten und über längere Zeit hinweg untersuchen können. Hierzu verwenden IDS üblicherweise mehr oder weniger umfangreiche Daten, die aus den verschiedenen überwachten Computersystemen und aus dem Netzwerk gewonnen werden. In diesen Daten sucht ein IDS Muster eines Angriffs oder auffällige Anomalien - und kann so wichtige Informationen liefern, um entweder einen aktuellen Angriff abzuwehren oder einen erfolgten Angriff zu analysieren. In jüngster Zeit haben IDS-Entwicklungen durch die neuen Methoden der künstlichen Intelligenz einen großen Schub erhalten. Eine umfangreiche und laufende Sammlung von Daten aus Systemen und Netzwerken erlaubt neben dem Einsatz von IDS-Systemen auch die Anwendung forensischer Verfahren, um einerseits vertiefte Erkenntnisse über einen erfolgten Einbruch zu erhalten. Damit können einerseits Maßnahmen für die zukünftige Abwehr abgeleitet werden, und andererseits die Grundlage für eine strafrechtliche Verwendung gelegt werden. In diesem Modul werden deshalb auch wichtige forensische Konzepte und Tools zu Themen der Speichertechnologien und der forensischen Datenanalyse und –wiederherstellung betrachtet. Es werden praktische Aspekte in den Bereichen Mobile, Smart Devices, Netzwerk und Cloud Forensik abgedeckt.
Verbindlichkeit	Pflicht innerhalb des gewählten Schwerpunkts Technik
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Assets und ihr Risikopotential - Intrusion Detection Systems (IDS) - Bewertung relevanter Daten und deren Erhebung - Filtern, Transformieren und Anreicherung von Daten - Anwendungsfälle der Analyse und Beispiele - Data Mining auf gesammelte Daten - Anwendungen der KI - Cyber-Angriffe und Krimimalität - Computer-Forensik: Daten-Analyse und Rekonstruktion - Netzwerk-Forensik: Angriffs-Rückverfolgung und Zuordnung

Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Casey, E. (ed.): Handbook of Digital Forensics and Investigation, Elsevier 2010 - Hu, F.: Security and Privacy in Internet of Things (IoTs), CRC Press 2016 - Northcutt S., Novak, J.: Network Intrusion Detection 3.Edition, New Riders 2003 - Sammons, J.: The Basics of Digital Forensics, Elsevier 2012
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

System- und Netzwerksicherheit - System and Network Security	
Modulnummer	CSMT2
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Prof. Dr. Jianmin Chen, weiter Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM2, CSM3, CSM4
Lernergebnisse des Moduls	Die Studierenden kennen aufbauend auf dem Modul „Systemanalse und Härtung“ Risiken und Schwachstellen von Systemen und Netzwerken. Zu den Netzwerken gehören Standard-IT-Netzwerke wie Local Area Network, Wireless Network, Cellular Network, Cellular Network, Internet, Intranet sowie die jüngeren Entwicklungen, wieRFID, NFC, WPAN und ZigBee im Consumer- und IoT-Bereich mit ihren spezifischen Architekturen sowie vor allem Risiko- und Sicherheitsbewertungen. Darüber hinaus werden spezielle Aspekte der Betriebstechnik und der kritischen Infrastruktur untersucht. Verschiedene Intrusionswerkzeuge und -methoden werden vorgestellt und für praktische Übungen genutzt. Maßnahmen zur Überwachung und Prävention von Angriffen werden in einer simulierten Umgebung trainiert.
Verbindlichkeit	Pflicht innerhalb des gewählten Schwerpunkts Technik
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Betriebsystemsicherheit - Sicherheitsaspekte von Netzwerken - Konzepte und Architekturen von Firewalls - Methodik von Angriffes und Gegenmaßnahmen - Sicherheit von mobile und cloud computing - Intrusion Detection und Prevention Systeme - Honeypots und Honeynets
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Stallings, W.: Cryptography and Network Security, 7.Editon, Pearson 2017 - Kizza, J.: Computer Network Security, Springer 2005 - Knapp, E.: Industrial Network Security,2. Edition, Elsevier 2015 - Vacca, J.(ed.): Network and System Security, Elsevier 2010
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Methoden der Künstlichen Intelligenz (KI)	
Modulnummer	**CSMT3**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Dr. Max Moser, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** keine
Lernergebnisse des Moduls	Die Studierenden erlangen einen fundierten Überblick über ausgewählte Bereiche der Künstlichen Intelligenz sowie praktische und methodische Kenntnisse und Fähigkeiten in der Anwendung von KI-Methoden und Algorithmen. Dies schließt die Fähigkeit zur Bewertung der Leistungsfähigkeit und Auswahl geeigneter Techniken für die jeweilige Problemdomäne ein. Sie können die Güte der Ergebnisse solcher Verfahren einschätzen.
Verbindlichkeit	Pflicht innerhalb des gewählten Schwerpunkts Technik
Modulinhalt	Die Veranstaltung umfasst u.a. folgende Themengebiete: - Überblick und Einführung - Intelligente Agenten - Repräsentation von Wissen und Problemen - Problemlösen durch Suchen, Adversariale Suche, Heuristiken - Wissen, Schließen, Planen - Unsicheres Wissen und Schließen - Maschinelles Lernen und Data Mining - Neuronale Netze - Lernen durch Verstärkung - Kommunizieren, Wahrnehmen und Handeln - Erfassen und Darstellen von typischen Software-Architekturen der KI - Entwicklung der Fähigkeit zur Anwendung dieser Methoden im Kontext von einfachen Problemstellungen. - Konzipieren und Implementieren von kleinen Agentenprogrammen. Im Rahmen der Übung werden die in der Vorlesung vorgestellten Methoden vertieft.
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Stuart Russell, Peter Norvig: Künstliche Intelligenz. Ein moderner Ansatz. Pearson Studium. 2012. - W. Ertel, Grundkurs Künstliche Intelligenz, Springer Vieweg, 2016 - George F. Luger: Artificial Intelligence. Structures and Strategies for Complex Problem Solving. Addison Wesley. 2004. - J. Kaplan, Künstliche Intelligenz: Eine Einführung, mitp Prefessional, 2017 - T. Rashid, F. Langenau, Neuronale Netze selbst programmieren, O'Reilly, 2017 - C.N. Nguyen, O. Zeigermann, Machine Learning – kurz & gut: Eine Einführung mit Python, Pandas und Scikit-Learn, O'Reilly, 2017 - G.D. Rey, K.F. Wender, Neuronale Netze: Eine Einführung in die

	Grundlagen, Huber, 2010 - I. Witten, E. Frank und M. Hall, Data Mining: Practical Machine Learning Tools and Techniques, 3. Auflage, Morgan Kaufmann (2011)
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des Moduls (in anderen Studiengängen)	Digitale Technologie (MA)
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Reifegradmodelle - Security Maturity	
Modulnummer	**CSMO1**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Dagmar Moser, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1
Lernergebnisse des Moduls	Die Studierenden wissen wie mittels standardisierter Verfahren die Evaluierung des vorhandenen Sicherheitslevels eines Unternehmens bzw. dessen Optimierung vorgenommen werden kann. Ziel dieser Standards ist es, Unternehmen und den Verantwortlichen für Security aktuelle und international anerkannte best-practices und Maßstäbe an die Hand zu geben, und so die (Weiter-)Entwicklung der Sicherheit eines Unternehmens zu verbessern. Die erwähnten Standards werden im Überblick und mit ausgewählten Fokus-Bereichen anhand von Praxisbeispielen besprochen. Insbesondere stellen die Themen Legacy Anwendungen, OT und kritische Infrastrukturen eine Herausforderung dar. Neben den etablierten und übergreifend einsetzbaren Standards soll ein Einblick in die z.B. in speziellen Branchen oder Ländern relevanten Anforderungen gegeben werden. Ergänzend werden wirtschaftliche Aspekte und Abwägungen (ROI, TCO,…) betrachtet.
Verbindlichkeit	Pflicht innerhalb des gewählten Schwerpunkts Organisation und Management

Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt:
	- Security-Maturity-Modelle und Standards - Motivation und Einsatz
	- Überblick und Diskussion ausgewählter Security-Maturity-Modelle, z.B.
	  - Common criteria
	  - BSIMM
	  - OWASP SAMM
	- Überblick und Diskussion wichtiger Security-Standards, z.B.
	  - NIST Framework
	  - ISO 2700x
	- Leistungskennzahlen (Key Performance Indicators -KPIs)
	- Beispielanwendungen und praktische Anwendungen

Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Common Criteria, https://www.commoncriteriaportal.org/cc/ - BSIMM https://www.bsimm.com/ - OWASP SAMM https://www.owasp.org/index.php/OWASP_SAMM_Project - NIST Framework https://www.nist.gov/cyberframework - ISO 2700X http://www.iso27001security.com/
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung	Bestandene MoP.

Vergabe von LP	
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Security Governance and Compliance	
Modulnummer	**CSMO2**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Franz Obermayer, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1
Lernergebnisse des Moduls	Die Studierenden kennen die Bedeutung einer Security Governance, die normative, strategische und organisatorische Rahmenbedingungen für die IT und speziell deren Sicherheitsaspekte zur Verfügung stellt. Sie strukturiert und präzisiert das sichere IT-Management und Informationsmanagement. Sie steht dabei im Spannungsfeld einer bestmöglichen Unterstützung der Unternehmensziele und - strategien durch die IT mit der Erzielung eines hohen Nutzwertes bei einer notwendigen Beachtung möglicher Risikopotenziale durch den Einsatz der IT (Sicherheit, Ausfall, Verstoß gegen Vorgaben). Die Studierenden kennen in diesem Kontext die Compliance mit dem primären Ziel, Entwicklung und Betrieb der IT unter Einhaltung und Beachtung spezifischer Gesetze, Richtlinien, Normen, Kodizes, Standards und Vertragswerke sicherzustellen. Die Compliance stellt die nachweisliche Einhaltung dieser Vorgaben gegenüber internen (Revision) und externen Institutionen (WP, Aufsichtsbehörden) sicher.
Verbindlichkeit	Pflicht innerhalb des gewählten Schwerpunkts Organisation und Management
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Einbettung der Information Security Governance in die Corporate Governance - Organisation und Struktur von Information Security Richtlinien - Aufgabe der Compliance und Kontrolle im Bereich der Security Governance - Risiko Management innerhalb einer Security Governance
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - von Solms, S.H.; von Solms, R.: Information Security Governance. Springer 2009 - ISO/IEC 27002 (2005). Information Technology – Security Techniques – Code of Practice for Information Security Management. ISO. www.iso.ch - COBIT (2005). Control Objectives for Information and Related Technology. ISACA. www.isaca.org
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des	

Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Sicherheitsmanagement - Security Manangement	
Modulnummer	**CSMO3**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Franz Obermayer, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1
Lernergebnisse des Moduls	Die Studierenden kennen den Aufbau und die Aufgaben des Informationssicherheits-Managements und Informationssicherheits-Managementsystems (englisch: Information Security Management System). Darüber werden geordnete Prozesse bzgl. des Umgangs mit den Problemstellungen der Informationssicherheit bereitgestellt.
Verbindlichkeit	Pflicht innerhalb des gewählten Schwerpunkts Organisation und Management
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Die Informationssicherheits-Organisation, mit Rollen und Ressourcen sowie Regelungen zur Verantwortung, - definierte Prozesse, in denen Risiken erfasst und bewertet werden (Risikomanagement mit Analyse von Gefährdungen und Angreifermodellen) sowie ein Sicherheitskonzept, in dem dokumentiert wird, welche Maßnahmen ergriffen werden sollen, um ein angestrebtes Sicherheitsniveau zu erreichen, - Maßnahmen, mit denen die Einhaltung der Sicherheitsvorgaben überprüft wird - Informationssicherheits-Management exemplarisch anhand der ISO-Standards 27001 und 27002
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Smith, C.; Brooks, D.: Security Science. Elsevier. Waltham 2013 - Schoenfield, B.: Securing Systems. CRC Press. Boca Raton 2015 - ISO/IEC 27002 (2005). Information Technology – Security Techniques – Code of Practice for Information Security Management. ISO. www.iso.ch
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Incident Management and Disaster Recovery	
Modulnummer	**CSM10**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Jianmin Chen
Dozent/en	Dr. Max Moser, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1, CSM2, CSM3, CSM4
Lernergebnisse des Moduls	Die Studiernden kennen den organisatorischen Ablauf im Umgang mit erkannten oder vermuteten Sicherheitsvorfällen sowie vorbereitende und ergänzende Maßnahmen und die jeweiligen Prozesse dazu. Durch diese Maßnahmen und Prozesse soll eine koordinierte Vorgehensweise aller Beteiligten ermöglicht werden, um nach Eintritt eines Security-Incidents Schaden vom Unternehmen abzuwenden, den betroffenen Service in der definierten Qualität wiederherzustellen und die Integrität der Unternehmensdaten und –Services zu gewährleisten. Hierbei sind organisatorische, rechtliche sowie technische Aspekte zu berücksichtigen. Die Studierenden kennen Regeln, Werkzeuge und Prozesse, die nach einem Security-Incident die Wiederaufnahme oder Fortführung unternehmenskritischer Prozesse, Applikationen und Infrastrukturen ermöglichen sollen. Grundlage für ein solches Desaster Recovery ist ein systematisches Assessment der relevanten Komponenten sowie eine Business-Impact-Analyse, die deren Business-Kritikalität bewertet.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten ermittelt: - Überblick und Motivation - Computer Emergency Response Teams - CERT - Organisation, Ausstattung und Kommunikation eines CERT - Incident-Prozesse - Incident Management Systeme (IMS) - Beispiele aus der Praxis und bekannte CERT-Organisationen - Desaster Recovery vs. Business Continuity Management - Business-Impact-Analyse - Störfallklassen und Kennzahlen für Krisenbewältigung - Organisatorische Vorbereitungen für Desaster Recovery und Einbettung in der Unternehmensorganisation - Guidelines von ISO, BSI und weitere Praxisbeispiele
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Rob Schnepp, Ron Vidal, Chris Hawley: Incident Management for Operations, O'Reilly - Matthew William Arthur Pemble, Wendy Fiona Goucher: The CIO's Guide to Information Security Incident Management, Auerbach Publications - Jamie Watters, Janet Watters: Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference, Apress-Verlag

	- Vacca, J.: Cyber Security and IT Infrastructure Protection. Syngress. Waltham 2014 - Griffor, E.: Handbook of Safety and Security, Syngress, Cambridge 2017 - Kostopoulos, G.: Cyberspace and Cybersecurity. CRC Press. Boca Raton 2013 - Computer Security Incident Handling Guide - NIST Special Publication 800-61R2
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen. Anhand von vorgegeben Fallbeispielen wird die Qualität der Projektarbeit sichergestellt.
Voraussetzung Vergabe von LP	Bestandene MoP
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Requirements Engineering and Threat Modelling	
Modulnummer	**CSM11**
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Dagmar Moser, weitere Dozenten nach Bedarf
Häufigkeit d. Angebots	Jedes Studienjahr
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Arbeitsaufwand (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Teilnahmeempfehlung	**Formal:** keine; **Inhaltlich:** CSM1
Lernergebnisse des Moduls	Die Studierenden kennen die große Bedeutung von Sicherheitsanforderungen im Requirements Engineering, welche häufig noch zu wenig beachtet werden. Sicherheitsanforderungen, die am Anfang eines Entwicklungsprojektes übersehen werden, werden meist gar nicht oder viel zu spät umgesetzt. Das führt zu Sicherheitslücken in Anwendungen, die im Nachhinein erhebliche Kosten verursachen können. In diesem Modul werden Grundlagen zum Requirements Engineering vermittelt; hierzu wird im Besonderen auf die Erhebung von Sicherheitsanforderungen eingegangen. Betrachtet werden funktionale genauso wie nicht-funktionale Anforderungen oder Anforderungen an die Architektur. Sicherheitsanforderungen lassen sich nur zum Teil mit Hilfe der gängigen Requirements Engineering Techniken (wie z.B. Fragetechniken) konkretisieren. Aus diesem Grund wird die Modellierung von Bedrohungen als eine spezielle Technik vorgestellt um Bedrohungen zu identifizieren und entsprechende Sicherheitsanforderungen daraus abzuleiten.
Verbindlichkeit	Pflicht
Modulinhalt	Im Rahmen der LV werden folgende Kenntnisse und Fähigkeiten vermittelt: - Grundlagen des Requirements Engineering, u.a. funktionale und nicht funktionale Anforderungen - Techniken zur Erhebung von Anforderungen - Modellierung von Bedrohungen - Ableitung von Sicherheitsanforderungen aus Bedrohungen
Literatur	**Eine abschließende Literaturauswahl wird durch den jeweiligen Dozenten vorgenommen.** - Basiswissen Sichere Software, Sachar Paulus, dpunkt-Verlag - Threat Modeling - Designing for Security, Adam Shostack, Wiley-Verlag - Basiswissen Requirements Engineering, Klaus Pohl, Chris Rupp, dpunkt-Verlag - Requirements- Engineering und -Management, Chris Rupp, Hanser Verlag
Sonstige Informationen	Arbeiten in Kleingruppen können einen Teil der Kontaktzeit ausmachen.
Voraussetzung Vergabe von LP	Bestandene MoP.
Verwendung des	

Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	Die Modulnote ist das gewogene arithmetische Mittel der Modulleistung(en). Die Gesamtnote der Master-Prüfung ist das gewogene arithmetische Mittel der Modulnoten und der Note der Abschlussprüfung. Die Gewichtung entspricht dabei in der Regel dem Anteil der LP (ECTS) an der Gesamtzahl von 90.

Masterthesis	
Modulnummer	CSMT
Themenbereich	Abschlussmodul
Dauer	1 Semester
Modulverantwortlicher	Prof. Dr. Sabine Rathmayer
Dozent/en	Individuell nach Thema festzulegen
Häufigkeit d. Angebots	Jedes Semester
LVF / SWS	SSt & KO
Arbeitsaufwand (WL)	600 h
LP (ECTS)	20 (18 LP: Masterthesis; 2 LP: Verteidigung)
MoP	HA & mP
Teilnahmeempfehlung	
Lernergebnisse des Moduls	Im Rahmen der Masterthesis sollen die Studierenden zeigen, dass Sie in der Lage sind - ein Thema konzeptionell umfassend und tiefgreifend zu behandeln - und die daraus gewonnen theoretischen Erkenntnisse auf eine praktische Unternehmensfragestellung anwenden können.
Internationaler und unternehmens-praktischer Bezug zum dualen Partnerunternehmen	Gemäß der Lernziele der HDBW ist im Rahmen der Masterthesis die Auseinandersetzung mit einem fachrelevanten Thema im internationalen Kontext besonders unterstützt. Ebenso ist die Arbeit in Zusammenarbeit mit Partnerunternehmen zu einer für das Unternehmen relevanten Fragestellung zu erstellen. Die Abstimmung des Themas für die Masterarbeit erfolgt zwischen betreuendem Professor, Studierendem und ggfs. Unternehmensvertreter.
Verbindlichkeit	Pflicht
Inhalt	Die Erstellung der Masterthesis besteht aus zwei Komponenten 1. Der selbständigen Erstellung einer Mastarbeit im Umfang von bis zu 80 Seiten. 2. Die Verteidigung und Präsentation der Ergebnisse der Masterarbeit mit einem Prüfungsgespräch, in dessen Rahmen die Inhalte der Masterarbeit auch in Verbindung zu sonstigen Inhalten des Studiums gesetzt werden. Die Dauer soll 10 Minuten nicht überschreiten. Die Gesamtdauer der Verteidigung darf 30 Minuten nicht überschreiten.
Sonstige Informationen	Die Anfertigung der Masterthesis kann in deutscher oder englischer Sprache erfolgen.
Voraussetzung Vergabe von Kreditpunkten	Bestandene Masterthesis und bestandene Verteidigung.
Verwendung des Moduls (in anderen Studiengängen)	
Stellenwert der Note für die Endnote	In diesem Fall geht die Bewertung der Masterthesis mit einer Gewichtung von 9/10 und die Bewertung der Verteidigung (KO) der Arbeit mit einer Gewichtung von 1/10 in die Note der Abschlussprüfung ein.

Index