

Technische Hochschule Brandenburg

Modulkatalog des Masterstudiengangs Security Management M. Sc. (Wahlpflichtmodule)

Verantwortlicher:

Prof. Dr. Ivo Keller, Studiendekan

Stand: Juli 2025

Impressum

Autor: Prof. Dr. Ivo Keller

Druck: Druckerei der Technischen Hochschule Brandenburg

Kontakt: Technische Hochschule Brandenburg

University of Applied Sciences

Magdeburger Str. 50

14770 Brandenburg an der Havel

T +49 3381 355 - 278

F +49 3381 355 - 199

E ivo.keller@th-brandenburg.de

www.th-brandenburg.de

Stand: Juli 2025

© Technische Hochschule Brandenburg

Inhaltsverzeichnis

Einleitung	4
1. Sprachmodelle und Neuronale Netze	7
2. Finetuning von LLMs.....	9
3. Penetration Testing	11
4. Cloud Security Strategy.....	13
5. Secure Data Center	15
6. Cyber Security.....	17
7. Angewandte Kryptographie	19
8. Technische Aspekte der IT-Forensik.....	21
9. OT-Sicherheit.....	24
10. Informationssicherheitsmanagementsysteme (ISMS)	26
11. Sicherheit der Energieerzeugung.....	28
12. Risikoanalysen und Risikomanagement.....	30
13. Business Continuity Management (BCM).....	32
14. Social Engineering	34

Einleitung

Dieses Dokument beschreibt die Wahlpflichtmodule (WPM) des Wahlpflichtfachs¹ des Masterstudiengangs *Security Management* der Technischen Hochschule Brandenburg in der Version der Studien- und Prüfungsordnung von 2023². Diese wird ergänzt durch die Eingangsprüfungsordnung für Berufserfahrene ohne Bachelorabschluss³.

Nach dem Regelstudienplan (Abb. 1) sind die drei vorgeschriebenen WPM im dritten Fachsemester begleitend zur Masterarbeit zu absolvieren. Die Studierenden können die WPM aber auch in den früheren Semestern belegen. Ein Wahlpflichtmodul geht über 2 SWS (22,5 Zeitstunden) und hat jeweils 3 ECTS ("Credit Points, CP"); insgesamt sind 3 WPM zu belegen. Wahlpflichtmodule dienen der Vertiefung und Spezialisierung, sie sind jeweils einem oder mehreren Profilrichtungen des Studiums zugeordnet.

Abbildung 1 Modulübersicht des Studiengangs Security Management

Sem	Module						Σ CP
1	Wissenschaftliches Schreiben (2 x 3 CP)	Netzwerksicherheit (6 CP)	Mathem.-techn. Grdl. der IT-Sicherheit (3 + 3 CP)	Sichere IKT-Infrastrukturen und IT-Dienste (2 x 3 CP)	Grundlagen des Security Managements (6 CP)	Recht, Compliance und Datenschutz (6 CP)	30
2		Projekt (6 CP)	Secure Systems Lifecycle Management (6 CP)		Security- und Krisenmanagement im internationalen Kontext ⁴ (6 CP)	Organisatorische Aspekte des Sicherheitsmanagements (3+3 CP)	30
3	Wahlpflichtmodul 1 (3 CP)		Wahlpflichtmodul 2 (3 CP)		Wahlpflichtmodul 3 (3 CP)		9
	Masterarbeit inkl. Kolloquium (21 CP)						21
							90

Lehrgebiet

Security Management
Recht und Betriebswirtschaftslehre
Mathematische und technische Grundlagen
IT-Sicherheit
Wissenschaftliches Arbeiten
Wahlpflicht

¹ *Fächer* sind Gruppen von *Modulen*. Module werden jeweils mit *einer* Prüfungsnote benotet und können aus mehreren Lehrveranstaltungen bestehen.

² SPO 2023 vom 13.12.2023, veröffentlicht am 26.03.2024 https://www.th-brandenburg.de/fileadmin/user_upload/hochschule/Dateien/Amtliche-Mitteilungen/2024/2024-01-SPO-MS-SECMan.pdf

³ EPO 2017 vom 18.10.2017, veröffentlicht am 19.01.2018: https://www.th-brandenburg.de/fileadmin/user_upload/hochschule/Dateien/Amtliche-Mitteilungen/2018/2018-04-EPO-SECMan.pdf

⁴ Pflichtfach für Wirtschaftsinformatik (M.Sc.)

Angebotene Wahlpflichtmodule und Profilrichtungen

In jedem Semester werden mindestens 2, oft bis zu 6 WPM angeboten, wobei jedes Semester geringfügige Änderungen im Angebot vorgenommen werden. Auf diese Weise kann die Verfügbarkeit der Dozenten berücksichtigt werden, auf aktuelle Entwicklungen eingegangen werden und das Lehrangebot weiterentwickelt werden. Die Tabelle 1 unten zeigt, welche WPM in welchem Semester angeboten werden. Der Tabelle 2 auf der Folgeseite ist zu entnehmen, welchen Profilrichtungen die WPM zugeordnet sind.

Tabelle 1: Verteilung der WPM über die Semester

Modul	Dozent	SoSe 2023	WiSe 2023	SoSe 2024	WiSe 2024	SoSe 2025	WiSe 2025
Sprachmodelle und Neuronale Netze	Prof. Dr. Ivo Keller					X	
Finetuning von LLMs	Prof. Dr. Ivo Keller					X	
Penetration Testing	Wilhelm Dolle	X					
Cloud Security Strategy	Johann Loran		(X)		X		X
Secure Data Center	Uwe Müller	X		X		X	
Cyber Security	Ingo Ruhmann	X		X		X	
Angewandte Kryptographie	Tilman Runge						
Technische Aspekte der IT-Forensik	Prof. Dr. Igor Podebrad						
OT-Sicherheit	Dan-Marvin Gluba	X					
Informationssicherheits-Managementssysteme (ISMS)	Sebastian Reinhardt		X		X		X
Sicherheit der Energieerzeugung	Prof. Dr. habil. Manfred Mertins				X		X
Risikoanalyse und Risikomanagement	Carsten Baeck		X		X		X
Business Continuity Management (BCM)	Holger Könnecke	X				X	
Social Engineering	Prof. Dr. Stephan Humer		X		X		X

Tabelle 2: Zuordnung der WPM zu den Vertiefungsrichtungen

Kursname	Dozent	Informationssicherheit	IT-Forensik	Business Continuity und Krisen-Management	IT und Cyber Security	Bankensicherheit	Gebäude-, Anlagen- und Personensicherheit
Sprachmodelle und Neuronale Netze	Prof. Dr. I. Keller	X	X	X	X	X	
Finetuning von LLMs	Prof. Dr. I. Keller	X	X	X	X	X	
Penetration Testing	Wilhelm Dolle	X	X		X	X	
Cloud Security Strategy	Johann Lorán	X	X		X	X	
Secure Data Center	Uwe Müller	X	X	X	X	X	X
Cyber Security	Ingo Ruhmann	X	X		X	X	
Angewandte Kryptographie	Tilmann Runge	X	X		X	X	
Technische Aspekte der IT-Forensik	Prof. Dr. I. Podebrád	X	X		X	X	
OT-Sicherheit	Dan-Marvin Gluba	X		X	X		X
Informationssicherheits- Managementsysteme (ISMS)	Sebastian Reinhardt	X		X	X	X	
Sicherheit der Energieerzeugung	Prof. Dr. habil. Manfred Mertins			X	X		X
Risikoanalyse und Risikomanagement	Carsten Baeck	X		X		X	X
Business Continuity Management (BCM)	Robert Osten/ Holger Könnecke	X	X	X	X	X	X
Social Engineering	Prof. Dr. S. Humer	X		X	X	X	X

1. Sprachmodelle und Neuronale Netze

Modul-Nr./Code:	SM602
WPM-Bezeichnung:	Sprachmodelle und Neuronale Netze
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	<ul style="list-style-type: none"> • SecMan Master, 1./2./3. Semester, WPM • Wirtschaftsinformatik-Master als Teil des WPMs „Predictive Analytics and Privacy“
Verwendbarkeit des Moduls:	<p>Dieses Modul kann für folgende Profilrichtungen verwendet werden:</p> <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • Business Continuity und Krisen-Management • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortlicher:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller
Lehrsprache:	Deutsch und ggf. Englisch
Voraussetzungen:	Grundlagen der Statistik, XML/HTML, Programmiererfahrungen in Java oder Python
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfung)
Lehrform/SWS:	Vorlesung: 30 Stunden
Studien-/ Prüfungsleistungen:	Hausarbeit und Referat, Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden Kompetenzen zur Modellierung und Klassifikation von Sprachmodellen. Sie benutzen dafür eine Programmier- und Visualisierungsumgebung wie z. B. Python oder Matlab. Die erworbenen fachlichen und methodischen Kompetenzen zielen auf den späteren Einsatz im Risikomanagement dem Operations Management und der Betrugserkennung ab.

Inhalte:	<p>Den Studierenden werden hierbei Kenntnisse zu folgenden grundlegenden Themenbereichen vermittelt:</p> <ul style="list-style-type: none"> • Natural Language Processing, Ontologien und Tokenizer • Word Embeddings, Gradienten und Optimierungsfunktionen • Maschinelles Lernen, Clusterung und Visualisierung, Deep Learning
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	<ul style="list-style-type: none"> • Chollet, F.: "Deep Learning with Python", 2018 • Duda, R. O., Hart, P. E., Stork D. G., "Pattern Classification", 2nd edition, John Wiley & Sons, New York, 2001 • Frochte, B.: "Maschinelles Lernen", 2019 • Keller, I., „Klassifikation in der Multimedia-Kommunikation“, Vorlesungsscript an der TU Berlin, Stand Juli 2014 • Klein, B.: „Numerisches Python: Arbeiten mit NumPy, Matplotlib und Pandas“, 2019
Besonderes:	//

2. Finetuning von LLMs

Modul-Nr./Code:	SM601
WPM-Bezeichnung:	Finetuning von LLMs
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	<ul style="list-style-type: none"> • SecMan Master, 1./2./3. Semester, WPM • Wirtschaftsinformatik Master als Teil des WPMs „Predictive Analytics and Privacy“
Verwendbarkeit des Moduls:	<p>Dieses Modul kann für folgende Profilrichtungen verwendet werden:</p> <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • Business Continuity und Krisen-Management • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortlicher:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller
Lehrsprache:	Deutsch
Voraussetzungen:	Modul „Sprachmodelle und Neuronale Netze“, Programmierungkenntnisse in Python
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfung)
Lehrform/SWS:	Vorlesung: 30 Stunden
Studien-/ Prüfungsleistungen:	Hausarbeit und Referat, Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	<p>Ziel dieser Lehrveranstaltung ist die Vermittlung der Grundlagen der Large Language Models, des Finetunings und der Integration eigener Wissensbestände.</p> <p>Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden eine grundsätzliche technologische Kompetenz hinsichtlich Generativer KI, ihrer fach- und sachgerechten Fähigkeiten sowie der Adaption an individuelle Interessenschwerpunkte im Risikomanagement, dem Operations</p>

	Management oder der Betrugserkennung.
Inhalte:	<p>Den Studierenden werden hierbei zu folgenden Themen Informationen vermittelt:</p> <ul style="list-style-type: none"> • Aktivierungsfunktion und Mehrfachklassifikation • Finetuning und Reinforcement Learning • Retrieval-Augmented Generation • Multi-head Attention • Nutzung der Sprachsynthese
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	<ul style="list-style-type: none"> • Brousseau, C., Sharp, M: LLMs in Production, ISBN 9781633437203, 2024 • Tunstall, L., von Werra, L., Wolf, T.: Natural Language Processing with Transformers, O'Reilly, 2022 • Manning, L.: Natural Language Processing with Deep Learning, Stanford University, 2024 • Kamath, U., Keenan, K., Somers, G., Sorenson, S.: Large Language Models: A Deep Dive, Springer Nature, 2024 • Weitere Literatur wird in der Vorlesung bekanntgegeben.
Besonderes:	//

3. Penetration Testing

Modul-Nr./Code:	SM2087
WPM-Bezeichnung:	Penetration Testing
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Dipl.-Chem. Wilhelm Dolle
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfung)
Lehrform/SWS:	Vorlesung: 30 Stunden
Studien-/ Prüfungsleistungen:	Hausarbeit und Referat, Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Bei Abschluss des Lernprozesses werden die Studierenden in der Lage sein, einen Penetrationstest mithilfe gängiger Hacking Tools nach Best-Practice-Vorgehensweise durchzuführen und zu dokumentieren. Gleichmaßen soll ein Verständnis dafür geschaffen werden, wie Ergebnisse eines Penetrationstests zu bewerten sind und welche Handlungsempfehlungen daraus resultieren. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz.

Inhalte:	<p>Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt:</p> <ul style="list-style-type: none"> • Kenntnisse über potenzielle Cyber-Risiken • Angreifertypen: Von Script Kiddies bis Advanced Persistent Threats • Vorstellung von Standards und Best-Practice-Ansätzen zur Durchführung von Penetrationstests • Rechtliche Rahmenbedingungen • Testverfahren und Aggressivität • Vorstellung gängiger Hacking Tools (Nmap, OWASP Zed, Metasploit, Nessus u. a.) • Live-Hacking • Durchführung eines Penetrationstests • Fundierte Einschätzung der Ergebnisse • Dokumentation und Handlungsempfehlungen • Advanced Cyber Defense
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	<ul style="list-style-type: none"> • Kevin R. Fall, W. Richard Stevens 2011: TCP/IP Illustrated Volume 1: The Protocols (978-0321336316) • Jon Erickson 2008: Hacking - Die Kunst des Exploits (978-3-89864-536-2) • Andrew S. Tannenbaum, David J. Wetherall 2012: Computernetzwerke (978-3-86894-137-1) • Holger Reibold 2015: Hacking Kompakt - Die Kunst des Penetration Testing (978-3-95444-161-7) • Michael Messner 2015: Hacking mit Metasploit – Das umfassende Handbuch zu Penetration Testing und Metasploit (978-3-86490-224-6)
Besonderes:	//

4. Cloud Security Strategy

Modul-Nr./Code:	SM2021
Modulbezeichnung:	Cloud Security Strategy
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 3. Semester, Wahlpflicht
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Dipl.-Inf. Johann Loran, M. Sc.
Lehrsprache:	Deutsch und Englisch
Voraussetzungen:	Grundlegendes Verständnis der Cloud-Konzepte und Cloud-Architekturen. Grundkenntnisse in der Entwicklung von Sicherheitsstrategien, IT-Sicherheitspraktiken und Risikomanagement. Es wird eine vorherige Teilnahme an den Vorlesungen "Unternehmensführung" und „Grundlagen des Security Managements“ empfohlen.
ECTS-Credits:	3
Gesamtworkload und seine Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfung)
Lehrform/SWS:	Vorlesung: 30 Stunden
Studien-/ Prüfungsleistungen:	Hausarbeit und Referat, Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	Laut SPO

Lernergebnisse:	<p>Nach erfolgreichem Abschluss dieses Wahlpflichtfachs besitzen die Studierenden folgende Kenntnisse:</p> <ul style="list-style-type: none"> • Entwickeln von Sicherheitsstrategien, -zielen und -maßnahmen, die speziell auf Cloud-Umgebungen zugeschnitten sind, • die wesentlichen Sicherheitsbedrohungen und -herausforderungen in Cloud-Umgebungen zu identifizieren und umzusetzen, • die Rolle eines Cloud Security Managers zu verstehen und effektiv in dieser Rolle zu agieren, • eine umfassende Cloud-Sicherheitsstrategie zu erstellen, zu präsentieren und zu verteidigen.
Inhalte:	<p>Den Studierenden werden vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt:</p> <ul style="list-style-type: none"> • Methoden und Good Practices zur Erstellung und Implementierung einer umfassenden Cloud-Sicherheitsstrategie, • Identifizierung, Bewertung und Management von Risiken und Bedrohungen in Cloud-Umgebungen, • Cloud Deployment-Modelle und Shared Responsibility Model, • Design und Implementierung sicherer Cloud-Infrastrukturen unter Berücksichtigung von Sicherheitsprinzipien und -konzepten, • IAM in Cloud-Umgebungen, • Cloud-Daten-, Plattform- und Infrastruktursicherheit, • sensitive Daten erkennen und klassifizieren, • DevSecOps und Anwendungssicherheit, • Überwachungs-, Auditierungs- und Security Incident Response-Praktiken für einen sicheren Betrieb der Cloud-Umgebung, • sichere Migration in eine Cloud, • regulatorische, Rechts- und Compliance-Grundlagen
Lehr- und Lernmethoden:	<p>Interaktiver Mix aus Vorlesung, Übungen in Kleingruppen und praktischen Übungen.</p>
Literatur:	<ul style="list-style-type: none"> • Fitzgerald, Todd (2020). CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers • Rumelt, Richard (2011). Good Strategy/Bad Strategy: The difference and why it matters • Porter, Michael E. (2004). Competitive Strategy: Techniques for Analyzing Industries and Competitors • Mulder, Jeroen (2023). Multi-Cloud Strategy for Cloud Architects • Finney, George (2022). Project Zero Trust: A Story about a Strategy for Aligning Security and the Business • Dotson, Chris (2023). Practical Cloud Security: A Guide for Secure Design and Deployment • Vehent, Julien (2018). Securing DevOps: Security in the Cloud • Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics • Ottenheimer, Davi (2012). Securing the Virtual Environment: How to Defend the Enterprise Against Attack • Haghighat, Mohammad (2015). CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications • NIST (2019). Guidelines on Security and Privacy in Public Cloud Computing

5. Secure Data Center

Modul-Nr./Code:	SM2083
Modulbezeichnung:	Secure Data Center: Kritikalität, Design, Operation
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • Business Continuity und Krisen-Management • IT und Cyber Security • Bankensicherheit • Gebäude-, Anlagen- und Personensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Dipl.-Ing. Uwe Müller
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit und Präsentation
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden Kenntnisse zur Kritikalität und zum Design von Data Centern. Daran anknüpfend werden Kenntnisse zum sicheren und effizienten Betrieb vermittelt. Inhaltlichen Schwerpunkt bilden Verfahren zur Analytik und Optimierung der Ausfallsicherheit von Data Centern. Die erworbenen fachlichen und methodischen Kompetenzen zielen auf die Vorbereitung für das Berufsleben ab.
Inhalte:	<ul style="list-style-type: none"> • Data Center: Richtlinien und normative Hintergründe • Risikoanalyse und Risikobewertung

	<ul style="list-style-type: none"> • Data Center Designs/Redesigns • Auswirkung organisatorischer, technischer, physischer und logischer IT-Sicherheit • Planung, Konzeption und Dimensionierung hinsichtlich: <ul style="list-style-type: none"> ○ Lage und Gebäude ○ Leistungs- und Platzbedarf ○ Zutrittsschutz und Einbruchschutz ○ Aktiver und passiver Brandschutz ○ Stromversorgung ○ Regelung der Umgebungsbedingungen ○ Kommunikations-Verkabelung ○ Redundanzkonzepte ○ Effizienz • Zuverlässigkeit, Verfügbarkeit, Fehlertoleranz, Resilienz • Nachhaltiger Betrieb und KPI's • Qualitative und quantitative Verfahren zur Zertifizierung
Lehr- und Lernmethoden:	<ul style="list-style-type: none"> • Vorlesung/Vorträge mit wechselnden Medien • Workshops in Kleingruppen • Geführte Inspektion von Data Centern
Literatur:	<ul style="list-style-type: none"> • Normenreihe DIN EN 50600 • BSI IT-Grundschutz-Kataloge • BITKOM Leitfaden „Betriebssicheres Rechenzentrum“ • Bernd Dürr, „IT-Räume und Rechenzentren planen und betreiben: Handbuch der baulichen Maßnahmen und Technischen Gebäudeausrüstung“, Verlag Bau + Technik • Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben
Besonderes:	Exkursionen zu Data Centern verschiedener Verfügbarkeitsklassen sind Bestandteil des Moduls.

6. Cyber Security

Modul-Nr./Code:	SM2092
Modulbezeichnung:	Cyber Security
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Dipl.-Inf. Ingo Ruhmann
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit und Präsentation Details werden zu Beginn des Kurses bekannt gegeben
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Bei Abschluss des Lernprozesses werden die Studierenden in der Lage sein, die Bedrohungen durch Cyberwar zu verstehen und verfügen über Kenntnisse zur Vorgehensweise und Methodik. Sie können die Wirksamkeit von Gegenmaßnahmen einschätzen. Mit den erworbenen Fähigkeiten sind die Studierenden in der Lage, eigene Lagebilder zu recherchieren und Gegenmaßnahmen vorzuschlagen. Die Studierenden beherrschen die theoretischen Grundlagen, um diese kognitiv, intuitiv und kreativ in der Studienarbeit umzusetzen.
Inhalte:	Den Studierenden werden vertiefte Kenntnisse zu folgenden Themen vermittelt:

	<ul style="list-style-type: none"> • Spezifika des Cyberwar im Vergleich zu anderen Manipulationsformen • Cybersecurity als Herausforderung für das Sicherheitsmanagement • Cybersecurity und der Schutz von KRITIS • Cyberwar aktuelle Fälle und Angriffstechniken • Cyberdefence-Strategien im Vergleich und Gegenstrategien
Lehr- und Lernmethoden:	<ul style="list-style-type: none"> • Vorlesung/ Vorträge mit wechselnden Medien (Beamer, Flipchart, Whiteboard) • Übungen in Kleingruppen und zusammen.
Literatur:	<ul style="list-style-type: none"> • https://ccdcoe.org/publication-library.html • Ingo Ruhmann: Cyberwar: Will it define the Limits to IT Security? In: IRIE - International Review of Information Ethics, Vol 20, 12/2013, S. 4-15 • Ingo Ruhmann, Ute Bernhardt: Information Warfare und Informationsgesellschaft. Zivile und sicherheitspolitische Kosten des Informationskriegs. In: Wissenschaft und Frieden, Heft 1/2014, Dossier Nr. 74 • Ingo Ruhmann: NSA, IT-Sicherheit und die Folgen. Eine Schadensanalyse ; in: Datenschutz und Datensicherheit, Heft 1, 2014, S. 40-46 • Ingo Ruhmann, Christiane Schulzki-Haddouti: Kryptodebatten. Der Kampf um die Informationshoheit; in: Christiane Schulzki-Haddouti (Hg.): Bürgerrechte im Netz, Bundeszentrale für politische Bildung, / Leske & Budrich, Bonn, 2003, S. 162-177 • Ingo Ruhmann: Rüstungskontrolle gegen den Cyberkrieg? In: Telepolis, 4.01.2010 • Ingo Ruhmann, Ute Bernhardt: Der EuGH-Entscheid als Anstoß für mehr Rechtssicherheit in der IT-Sicherheit; in: DuD, Nr. 1, 2017, S. 34-38 • Ingo Ruhmann, Ute Bernhardt: Information Warfare – From Doctrine to Permanent Conflict; in: Christian Reuter (Hg.): Information Technology for Peace and Security; IT Applications and Infrastructures in Conflicts, Crises, War, and Peace, Springer Fachmedien, 2019 • Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann, Dieter Wöhrle: Naturwissenschaft - Rüstung - Frieden Basiswissen für die Friedensforschung, VS-Verlag, 2. überarbeitete Auflage, 2017 <p>Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.</p>
Besonderes:	//

7. Angewandte Kryptographie

Modul-Kurzkennzeichen:	SM2101
Modulbezeichnung:	Angewandte Kryptographie
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • IT- und Cybersecurity • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Tilman Runge, M. Sc.
Lehrsprache:	Deutsch und Englisch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Mündliche Prüfung in Verbindung mit Hausarbeit und Präsentation. Die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	Lt. SPO
Lernergebnisse:	Ziel dieser Lehrveranstaltung ist es, die Lernenden dazu zu befähigen, Managementkompetenzen zu entwickeln und im beruflichen Kontext gezielt einzusetzen – insbesondere in Bereichen, in denen kryptographisches Wissen zur Bewertung und Steuerung von Sicherheitsmaßnahmen erforderlich ist. Dies betrifft unter anderem:: <ul style="list-style-type: none"> • Entscheidungskompetenz bei der Auswahl und dem Einsatz von Systemen, deren Sicherheit auf kryptographischen Verfahren beruht • Beurteilungskompetenz bei der Auditierung von Anwendungen und Systemen, die Kryptographie implementieren • Risikoabschätzung beim Einsatz von Kryptographie in Bezug auf den "Quantum Threat"

	<ul style="list-style-type: none"> • Vertiefung des kryptographischen Grundlagenwissens •
Inhalte:	<p>Im Modul wird der Einsatz von Kryptographie in populäreren Internetanwendungen aus einer Managementperspektive analysiert. Die Inhalte werden anhand von Anwendungen erarbeitet, mit denen Studierenden aus privatem und beruflichen Alltag vertraut sind. Die Modulthemen beinhalten:</p> <ul style="list-style-type: none"> • Verschlüsselung bei Instantmessengern: Whatsapp, Signal und Telegram • Herausforderungen sicheren Webbrowsers bei der Nutzung von HTTPS/TLS • E-Mailverschlüsselung mittels S/MIME und PGP • Kryptographie in Hardware am Beispiel von Chipkarten, Hardware Security Modules (HSM) und Trusted Computing • Verteilte Internetanwendungen wie Blockchain und TOR • Bedrohung von Kryptographie durch Quantencomputer (Quantum Threat) •
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen, Vorstellung von Praxisbeispielen, technische Übungen am eigenen Laptop
Literatur:	<ul style="list-style-type: none"> • Wolfgang, H., Fritz, R.: „Nicht hackbare Rechner und nicht brechbare Kryptographie“, Springer Vieweg 2018 • Singh, S.: „Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets“, dtv Verlagsgesellschaft, 2001 • Beutelspacher, A., Schwenk, J., Wolfenstetter, K.-D.: „Moderne Verfahren der Kryptographie“, Springer Spektrum 2015 • Davies, J.: „Implementing SSL/TLS“, Wiley Publishing 2011 • Schwenk, J.: „Sicherheit und Kryptographie im Internet“, Springer Vieweg, 2014 • Ristić, J.: „Bulletproof SSL and TLS“, Feisty Duck, 2017
Besonderes:	Das Modul Angewandte Kryptographie bereitet die Studierenden auf die kryptographierelevanten Inhalte der Zertifizierungen Certified Information Systems Security Professional (CISSP) und Certified Information Systems Manager (CISM) vor.

8. Technische Aspekte der IT-Forensik

Modul-Nr./Code:	SM2007
Modulbezeichnung:	Technische Aspekte der IT-Forensik
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Igor Podebrad
Dozent/in:	Prof. Dr. Igor Podebrad
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit und Präsentation
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Die Studierenden sind in der Lage, die Kenntnisse und Fertigkeiten zu IT-forensischer Vorgehensweisen und technischer Analysemethoden einzusetzen. Die Studierenden führen IT-forensische Untersuchungen am Beispiel zweier unterschiedlicher Filesysteme durch und können diese anwenden. Sie beherrschen die theoretischen Grundlagen, um diese kognitiv, intuitiv und kreativ in der Studienarbeit umzusetzen.
Inhalte:	Den Studierenden werden vertiefte Kenntnisse zu Grundsätzen und Anforderungen, speziell im internationalen Kontext und vor dem Hintergrund unterschiedlicher rechtlicher Situationen, vermittelt: <ul style="list-style-type: none"> • Datenträgeranalyse <ul style="list-style-type: none"> • Übersicht Typen von Festplatten (SCSI, xATA, xIDE, etc.) • Übersicht physische Aufteilung einer Platte (cylinder, head, sector) • Übersicht logische Aufteilung einer Platte (partitions, raw data) • Übersicht Dateisysteme (FAT, NTFS als Schwerpunkt, ggfls.)

	<ul style="list-style-type: none"> ext2, ext3) • Übersicht Dateiverwaltung (Cluster, slack space [drive slack, RAM slack) • Details Festplattenanalyse (Sicherheitsmaßnahmen, tools, hands on) • Dateien und ihre Eigenschaften (Metadaten) • Arten von Dateien (normal, hidden, deleted, encrypted, alternate datastream) • string search (logisch vs. physisch, Kodierung) • Details FAT • Historische FAT-Systeme (FAT 12, FAT 16) • FAT32 (Strukturen, Namenskonvention) • Betriebssystemanalyse <ul style="list-style-type: none"> • Server vs. Workstation • Lokation OS auf Platte • Prozessanalyse • Netzwerkverbindungen • Registry • NTFS (Metadaten und Details) • Details Alternate Datastreams • Details Filetypen • Windows-Artefakte (cookies, temporary files, MRU, print jobs) • timelining • Details Registry • Email-Analyse • Netzwerkanalyse <ul style="list-style-type: none"> • Grundlagen • Protokolle • Detail-Analyse • Anomalien • verdeckte Kommunikation • Angriffstypen
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	<ul style="list-style-type: none"> • File System Forensic Analysis, Brian Carrier, Taschenbuch: 600 Seiten, Verlag: Addison-Wesley Longman, Amsterdam (17. März 2005), Sprache: Englisch, ISBN-10: 0321268172, ISBN-13: 978-0321268174 • Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, Alexander Geschonneck, Broschiert: 342 Seiten, Verlag: dpunkt Verlag; Auflage: 4., aktualisierte Auflage (22. Februar 2010), Sprache: Deutsch, ISBN-10: 3898646580, ISBN-13: 978-3898646581 • Windows® Internals, Fifth Edition (PRO-Developer), Mark Russinovich & David A. Solomon, Gebundene Ausgabe: 1232 Seiten, Verlag: Microsoft Press; Auflage: Fifth Edition. (17. Juni 2009), Sprache: Englisch, ISBN-10: 9780735625303, ISBN-13: 978-0735625303, ASIN: 0735625301 • Harlan Carvey, Windows Forensic Analysis, Verlag: Syngress Media; Auflage: 2nd edition. (13. Juli 2009), ISBN-13: 978-1597494229 • Sammes; Jenkinson, Forensic Computing: A Practitioner's Guide, Verlag: Springer, Berlin; Auflage: 2nd ed. (30. Juli 2007), ISBN-13: 978-1846283970

Besonderes:	//
-------------	----

9. OT-Sicherheit

Modul-Nr./Code:	SM2102
Modulbezeichnung:	OT-Sicherheit
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflicht
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • IT und Cyber Security • Business Continuity und Krisen-Management • Gebäude-, Anlagen- und Personalsicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Dan-Marvin Gluba, M.A.
Lehrsprache:	Deutsch und Englisch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und seine Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS	Vorlesung: 2SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit und Präsentation
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Wahlpflichtmoduls kennen die Studierenden die wesentlichen Merkmale und Komponenten von industriellen Steueranlagen, deren Funktionsweise und Kritikalität innerhalb der Gesellschaft. Darüber hinaus erlangen sie Kenntnisse, welche Anforderungen erfüllt sein müssen, um diese Anlagen vor potentiellen physikalischen, wie auch Cyber-Angriffen zu schützen.
Inhalte	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: <ul style="list-style-type: none"> • OT Spezifika (Komponenten, Protokolle, etc.) • Aktuelle Bedrohungslage innerhalb der OT-Security • Allgemeine OT-Security Regularien • Industriespezifische Normen • IoT/IIoT Normen und Standards
Lehr- und Lernmethoden:	Interaktive Mischung aus Vorlesung, Übungen in Kleingruppen und praktische Übungen
Literatur:	<ul style="list-style-type: none"> • NIST SP 800 series

	<ul style="list-style-type: none"> • ISO/IEC 62443 • Bundesamt für Sicherheit in der Informationstechnik, ICS-Security-Kompodium (2013). • Christopher Tebbe, M.Sc., Durchgängiges Wissensmanagement von OT-Security Wissen im Lebensweg von Produktionsanlagen (Hamburg 2021). • Sebastian Rohr, Industrial IT Security- Effizienter Schutz vernetzter Produktionslinien (Februar 2019) • Edward J.M. Colbert, Alexander Kott (Hrsg.), Cybersecurity of SCADA and Other Industrial Control Systems, Advances in Information Security Band 66 (Juni 2018).
Besonderes:	//

10. Informationssicherheitsmanagementsysteme (ISMS)

Modul-Nr./Code:	SM2004
Modulbezeichnung:	Informationssicherheitsmanagementsysteme (ISMS)
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • Business Continuity und Krisen-Management • IT und Cybersecurity • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Sebastian Reinhardt, M. Sc., Marie-Luise Troschke, M. Sc.
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit und Präsentation
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach dem Modul können die Studierenden verschiedene Anforderungen an ein Information-Security Management System verstehen sowie die Standards ISO27001 und BSI-Grundschutz anwenden. Die Lernenden sollen die methodischen Fähigkeiten zur Analyse, Bewertung; und Vorschläge von Maßnahmen sowie das Implementieren eines ISMS in einem Unternehmen trainieren. Mit den erworbenen Kenntnissen sind die Studierenden in der Lage ein eigenständiges ISMS-Konzept zu erstellen. Die erworbenen fachlichen und methodischen Kompetenzen zielen auf die Vorbereitung für das Berufsleben ab.

Inhalte:	<p>Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt:</p> <ul style="list-style-type: none"> • ISO 27001 und ff. • BSI IT-Grundschutz • Unterschiede und Gemeinsamkeiten • Erfolgsfaktoren bei der Umsetzung
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	<ul style="list-style-type: none"> • BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) • BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) • BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise • BSI-Standard 200-2: IT-Grundschutz-Methodik • BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz • BSI-Standard 200-3: Risikomanagement • BSI IT-Grundschutz-Kataloge in der aktuellen Ergänzungslieferung
Besonderes:	//

11. Sicherheit der Energieerzeugung

Modul-Nr./Code:	SM2089
Modulbezeichnung:	Sicherheit der Energieerzeugung
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Business Continuity und Krisen-Management • IT- und Cyber Security • Gebäude-, Anlagen- und Personensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr.-Ing. habil. Manfred Mertins
Dozent/in:	Prof. Dr.-Ing. habil. Manfred Mertins
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS
Studien-/Prüfungsleistungen:	Hausarbeit und Referat/Präsentation, bzw. mündliche Prüfung; die genaue Prüfungsform wird vor Beginn der Lehrveranstaltung bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Bei Abschluss des Lernprozesses werden die Studierenden Kenntnisse und Fertigkeiten erlangt haben, die ihnen eine Übersicht über die bei der Bewertung der Sicherheit der Energieerzeugungsprozesse heranzuziehenden Bedrohungen, Stör- und Unfällen vermittelt. Dafür werden Methoden zur Bewertung von Gefährdungen der kritischen Infrastruktur „Energie“ infolge naturbedingter oder zivilisationsbedingter Einwirkungen vorgestellt und eine Übersicht über Sicherheitskonzepte für Einrichtungen zur Energieerzeugung mit Bedeutung für Konzepte zum Schutz kritischer Infrastrukturen, Schwerpunkt „Gestaffeltes Sicherheitskonzept“ gegeben. Die Studierenden werden Prüfkonzepte zur Sicherstellung und zum Erhalt erforderlicher Qualitätsmerkmale bei Fertigung, Errichtung und Betrieb von Einrichtungen zur Energieerzeugung einschließlich

	<p>Anwendung auf kritische Infrastrukturen kennenlernen, Methoden zur Schwachstellenanalyse und Auswertung von Betriebserfahrungen und den Umgang mit Abweichungen von normativen Vorgaben, Bewertung der sicherheitstechnischen Bedeutung von Abweichungen. Eine Übersicht über internationale und nationale Vorschriften zur Definition aktueller und künftiger naturbedingter und zivilisationsbedingter Einwirkungen auf Einrichtungen der Energieerzeugung wird vorgestellt. Die Bewertung von Bedrohungen aus einer globalisierten Welt für die Integrität kritischer Infrastrukturen wird diskutiert. Aktuelle Sachverhalte aus der Umsetzung der Energiewende im Hinblick auf die Versorgungssicherheit und Umweltverträglichkeit der Stromversorgung in Deutschland und in der EU werden behandelt. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz.</p>
Inhalte:	<p>Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt:</p> <ul style="list-style-type: none"> • Analyse von Stör- und Unfällen mit Bedeutung für kritische Infrastrukturen, insbesondere für Einrichtungen zur Energieerzeugung • Anwendung deterministischer und probabilistischer Analysemethoden zur Bewertung der sicherheitstechnischen Bedeutung von Betriebserfahrungen sowie neuen Erkenntnissen für die Integrität und Funktionsweise kritischer Infrastrukturen • Konzepte zum Schutz gegen sonstige Einwirkungen Dritter (SEWD) • Differenzierung der Begriffe „(Nuclear) Safety“ und „(Nuclear) Security“, Erläuterung der Synergien • Maßnahmen zur Sicherstellung der Qualität bei Fertigung, Errichtung und Betrieb kritischer Infrastrukturen • Differenzierung und Erläuterung der Begriffe „naturbedingte“, „zivilisationsbedingte“ und „sonstige Einwirkungen Dritter“ sowie Ableitung für die Sicherheitsstrategie • Normative Vorgaben in Deutschland sowie internationale Empfehlungen, Bedeutung europäischer Regelsetzungen unter Berücksichtigung des Standes von Wissenschaft und Technik
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	<ul style="list-style-type: none"> • Safety and Security Publications der IAEA in Wien • Publikation des BBk zum Thema "Kritische Infrastrukturen" • Publikationen aus dem Sicherheitsforschungsprogramm der Bundesregierung „Sicherheitsforschung - Forschung für die zivile Sicherheit“ • Publikationen von WENRA (Western European Nuclear Regulators Association) u. a. • Winje, Witt: Energiewirtschaft, Springerverlag 2013 • Zahoransky, Fichter: Energietechnik, Systeme zur konventionellen und erneuerbaren Energieumwandlung, Springer Vieweg 2024 • Laufs: Reaktorsicherheit für Leistungskernkraftwerke, Springerverlag 2013.
Besonderes:	//

12. Risikoanalysen und Risikomanagement

Modul-Nr./Code:	SM2010
Modulbezeichnung:	Risikoanalyse und Risikomanagement
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • Business Continuity und Krisen-Management • Bankensicherheit • Gebäude-, Anlagen- und Personensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Carsten Baeck
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS
Studien-/Prüfungsleistungen:	Hausarbeit und Präsentation oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Bei Abschluss des Lernprozesses werden die Studierenden in der Lage sein, Risiken nach verschiedenen Methoden zu analysieren und zu bewerten. Sie sind in der Lage, die verschiedenen Methoden sowie deren Ergebnisse einzuschätzen und anzuwenden. Sie beherrschen die theoretischen Grundlagen und entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz.
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt: <ul style="list-style-type: none"> • Verschiedene Ansätze der Risikoanalyse • Probabilistische und deterministische Ansätze • Retrospektive und prospektive Analysen

	<ul style="list-style-type: none"> • Qualitative und quantitative Ansätze • Umgang mit Unsicherheiten • Ansätze aus dem Qualitätsmanagement, bzw. der Sicherheitsbewertung technischer Systeme • Management von Risiken in verschiedenen Umgebungen • Etablierte Frameworks des Risikomanagements
Lehr- und Lernmethoden:	<ul style="list-style-type: none"> • Vorlesung/ Vorträge mit wechselnden Medien (Beamer, Flipchart, Whiteboard) • Übungen in Kleingruppen und zusammen
Literatur:	<ul style="list-style-type: none"> • British Standard - 25999: Business Continuity Management [Buch], London, 2006 • Brühwiler Bruno - Risikomanagement als Führungsaufgabe: ISO 31000 mit ONR 49000 wirksam umsetzen [Buch], 2011 • Brühwiler Bruno und Romeike Frank - Strategische Früherkennung [Buch], 2010 • http://www.controllingwiki.com/de/index.php/Risikoanalyse_FMEA. • Dornes Nadeshda - Alternative Risikomodellierungs-, Risikoanalyse- und Bewertungsmethode: Risikomanagement ohne komplexe mathematische Modelle [Buch], Hamburg, disserta Verlag, 2014 • eurorisk.ch [Online], http://www.eurorisk.ch/.fh-hannover.de, 2015 http://transfer.tr.fhhannover.de/projekte/norma/pix/glossar/risiko_wahrnehmung.htm • http://www.es.hsmannheim.de/sps/Uebungen/Kapitel8/Uebung8_2.html • maschinenrichtlinie-2006-42-eg.de [Online], 2015, http://www.maschinenrichtlinie-2006-42-eg.de/grunds%C3%A4tze-der-risikobeurteilung-von-maschinen • ONR 49000, 2010 • ONR 49002-1, 2010 • ONR 49002-2, 2010 • orghandbuch.de [Online], 2015 http://www.orghandbuch.de/OHB/DE/Organisationshandbuch/6_MethodenTechniken/63_Analysetechniken/633_FehlermoeglichkeitUndEinflussanalyse/fehlermoeglichkeitundeinflussanalysenode.html. • pwc.de [Online], 2015, http://www.pwc.de/de/risiko-management/studie-offenbart-maengel-imrisikomanagement-deutscher-unternehmen.jhtml . • risikomanager.org [Online], 2015, http://risikomanager.org/methodenassistent/fehlerbaumanalyse/.risknet.de [Online], 2015 • Romeike Frank und Hager Peter - Erfolgsfaktor Risiko-Management 3.0: Methoden, Beispiele, Checklisten Praxishandbuch für Industrie und Handel [Buch], Wiesbaden: Springer Gabler, 2013
Besonderes:	//

13. Business Continuity Management (BCM)

Modul-Nr./Code:	SM2085
Modulbezeichnung:	Business Continuity Management (BCM)
ggf. Aufteilung in Lehrveranstaltungen:	Nein
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • IT-Forensik • Business Continuity und Krisen-Management • IT und Cyber Security • Bankensicherheit • Gebäude-, Anlagen- und Personensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Robert Osten
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS
Studien-/ Prüfungsleistungen:	Hausarbeit oder Referat/Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden Kenntnisse über den Aufbau eines BCM nach ISO 22301 und die Einbettung in die Unternehmensorganisation, sowie die Verzahnung des BCM mit dem Informations-Sicherheitsmanagement (ISMS). Dafür werden Fähigkeiten vermittelt, um kritische Geschäftsprozesse und Infrastrukturen zu identifizieren und die Auswirkungen von Vorfällen, Minimieren der Ausfallzeiten und verkürzen der Wiederherstellungszeit. Die Studierenden trainieren durch die gestellten Aufgaben ihre Teamfähigkeit und ihr Selbstmanagement.

Inhalte:	<p>Den Studierenden werden vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt:</p> <ul style="list-style-type: none"> • Aufbau eines BCM nach ISO 22301 • Einbinden des BCM in Unternehmensorganisation allgemein und die Sicherheitsorganisation im Speziellen. • Schnittstellen zum Informationssicherheitsmanagement, zum Risikomanagement, zur Notfallplanung und weiteren Bereichen der Unternehmenssicherheit. • Kernbegriffe und Grundkonzepte im BCM • Prozessmodellierung und Identifikation kritischer Geschäftsprozesse, kritischer Infrastrukturen, Versorgungsketten und Zulieferer • Modellierung von (und Umgang) mit Interdependenzen
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	<ul style="list-style-type: none"> • Disaster Recovery, Crisis Response, and Business Continuity A Management Desk Reference //by: Watters, Jamie Berkeley, CA; s.l., Apress, 2014 Volltext: https://ezproxy.th-brandenburg.de/login?url=http://dx.doi.org/10.1007/978-1-4302-6407-1 • Business Continuity: Notfallplanung für Geschäftsprozesse (Xpert.press) // von: Martin Wieczorek, Uwe Naujoks und Bob Bartlett (Hrsg.); Berlin / Heidelberg; Springer 2003 • http://www.bcm-institute.org/ • Business Continuity Management by Patrick Woodman 2007 • International Journal of Business Continuity and Risk Management: http://www.inderscience.com/jhome.php?jcode=ijbcrm
Besonderes:	//

14. Social Engineering

Modul-Nr./Code:	SM2012
Modulbezeichnung:	Social Engineering
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: <ul style="list-style-type: none"> • Informationssicherheit • Business Continuity und Krisen-Management • IT und Cyber Security • Bankensicherheit • Gebäude-, Anlagen- und Personensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Stephan G. Humer
Dozent/in:	Prof. Dr. Stephan G. Humer
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS
Studien-/Prüfungsleistungen:	Hausarbeit und Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach Absolvierung des Moduls können die Studierenden verschiedene psychologische und soziologische sowie digitale Ansätze von Social Engineering, insbesondere die komplexen gegenwärtigen Sicherheitsherausforderungen im Rahmen von Krisen, Kriegen und KI („Social Engineering 2.0“), zielführend analysieren, einordnen und in ihrem Arbeitskontext zur Abwehr und für erste Schulungsideen einsetzen. Den Studierenden werden Möglichkeiten und Grenzen der sozialen Manipulation insbesondere in digitalen Umgebungen aufgezeigt. Des Weiteren werden die historischen, politischen und gesellschaftlichen Hintergründe des Themenfelds beleuchtet. Die Studierenden kennen am Ende des Moduls die theoretischen und

	praktischen Grundlagen, um diese kognitiv, intuitiv und kreativ in der Studienarbeit entweder für ein Abwehr- und/oder Awareness-Konzept umzusetzen.
Inhalte:	Das Seminar basiert auf dem 3A-Ansatz: Angriff, Abwehr, Awareness. Die Studierenden lernen Theorie, Methoden und Praxis von Social-Engineering-Angriffen kennen, um daraus Abwehrstrategien zu entwickeln. Anschließend werden Awarenesskonzepte diskutiert, um erste eigene Schulungsansätze zu entwerfen. Dabei werden insbesondere gegenwärtige Herausforderungen diskutiert sowie Ansätze der Themen von übermorgen in methodischer Hinsicht aufgegriffen.
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	<ul style="list-style-type: none"> • <p>Lahmer, N.: Social Engineering – Die neuen Angriffsstrategien der Hacker. Redline Verlag, 2022.</p> <p>Lardschneider, M.: Social Engineering. Eine ungewöhnliche aber höchst effiziente Security Awareness Maßnahme. DuD 9/2008, S. 574-578. https://link.springer.com/content/pdf/10.1007/s11623-008-0137-1.pdf</p> <p>Loewe-Baur, M. (2021). Social Engineering - Der Mensch als Einfallstor. In: Schwarzenegger, Christian; Nägeli, Rolf. Schwachstelle Mensch : Prävention gegen alte und neue Formen der Kriminalität: 12. Zürcher Präventionsforum: Tagungsband 2021. Zürich: EIZ Publishing, 9-36. https://www.zora.uzh.ch/id/eprint/223547/1/Loewe_Baur_Social_Engineering.pdf</p> <p>Schreier, M., Stöckli, P., Annen, H.: Social Engineering im militärischen Kontext. Allgemeine Schweizerische Militärzeitschrift, 07/2021, S. 40-41. https://www.asnz.ch/fileadmin/asnz/Dokumente/Juli%202021/Social%20Engineering%20im%20milit%C3%A4rischen%20Kontext.pdf</p> <p>Schumacher, S.: Die psychologischen Grundlagen des Social Engineerings. Information. Wissenschaft & Praxis 2014; 65(4–5): 215–230. https://doi.org/10.1515/iwp-2014-0039</p> <p>Suker, M.: Das Social Engineering Dilemma: Warum Organisationen trotz Schulungsmaßnahmen Opfer von Social Engineering Angriffen werden. S. 195-204. In: Alexa, A. (Hrsg.): Streitkräfte Quo Vadis. Tagungsbald der Militärwissenschaftlichen Tagung 2022 „Militär.Schafft.Wissen.“ Schriftenreihe der Landesverteidigungsakademie. 3/2023. https://www.bmlv.gv.at/pdf_pool/publikationen/03_2023_s_ihmf_streitkraefte_quo_vadis_webversion_v2.pdf</p>
Besonderes:	Aktuelle Hinweise zum Seminar regelmäßig unter https://www.humer.de

