Technische Hochschule Brandenburg
University of Applied Sciences

Technische Hochschule Brandenburg

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

Verantwortlicher:
Prof. Dr. Ivo Keller, Studiendekan

Stand: Oktober 2022

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:	Oktober 2022

Inhaltsverzeichnis

Einleitung

Dieses Dokument beschreibt die Wahlpflichtmodule (WPM) des Wahlpflichtfachs[1]des Masterstudiengangs *Security Management* der Technischen Hochschule Brandenburg in der Version der Studien- und Prüfungsordnung von 2017[2]. Diese wird ergänzt durch die Eingangsprüfungsordnung für Berufserfahrene ohne Bachelorabschluss[3].

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 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

<table>
<tr><th>Sem</th><th colspan="7">Module</th><th>∑ CP</th></tr>
<tr><td>1</td><td rowspan="2">Wissen-schaft-liches Schrei-ben (2 x 3 CP)</td><td>Netzwerksicherheit (6 CP)</td><td colspan="2">Mathem.-techn. Grdl. der IT-Sicherheit (3 + 3 CP)</td><td rowspan="2">Sichere IKT-Infra-struk-turen und IT-Dienste (2 x 3 CP)</td><td>Grundlagen des Security Managements (6 CP)</td><td>Recht, Compliance und Datenschutz (6 CP)</td><td>30</td></tr>
<tr><td>2</td><td>Projekt (6 CP)</td><td colspan="2">Secure Systems Lifecycle Management (6 CP)</td><td>Security- und Krisenmanagement im internationalen Kontext[4] (6 CP)</td><td>Organisatorische Aspekte des Sicherheits-managements (3+3 CP)</td><td>30</td></tr>
<tr><td rowspan="2">3</td><td colspan="3">Wahlpflichtmodul 1 (3 CP)</td><td colspan="2">Wahlpflichtmodul 2 (3 CP)</td><td>Wahlpflichtmodul 3 (3 CP)</td><td>9</td></tr>
<tr><td colspan="6">Masterarbeit inkl. Kolloquium (21 CP)</td><td>21</td></tr>
<tr><td></td><td colspan="7"></td><td>90</td></tr>
</table>

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 2017 vom 18.10.2017, veröffentlicht am 19.01.2018: https://www.th-brandenburg.de/fileadmin/user_upload/hochschule/Dateien/Amtliche-Mitteilungen/2018/2018-05-SPO-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 2020	WiSe 2020	SoSe 2021	WiSe 2021	SoSe 2022	WiSe 2022
Predictive Analytics	Prof. Dr. Ivo Keller	X		X		X	
Datensicherheit in der vernetzten Welt	Prof. Dr. Ivo Keller	X		X		X	
Penetration Testing	Wilhelm Dolle	~~X~~		X		X	
Cloud Security	Johann Loran		X		X		X
Secure Data Center	Uwe Müller	X		X		X	
Cyber Security	Ingo Ruhmann	X		X		X	
Angewandte Kryptographie	Tilmann Runge	X		X	X		
Technische Aspekte der IT-Forensik	Prof. Dr. Igor Podebrad		X		X		
OT-Sicherheit	Dan-Marvin Gluba, Lars Schmidt						X
Sicherheit im BOS-Umfeld	Prof. Dr. Walter Gora		X			X	
Informationssicherheits-Managementsysteme (ISMS)	Sebastian Reinhardt, Lars Schmidt		X		X		X
Sicherheitstechnische Begutachtung kritischer Infrastrukturen (KRITIS)	Prof. Dr. habil. Manfred Mertins		X		X		X
Risikoanalyse und Risikomanagement	Carsten Baeck		X		X		X
Business Continuity Management (BCM)	Prof. Dr. Oliver Weissmann		X		X	X	
Social Engineering	Prof. Dr. Stephan Humer		X		X		X
Personenschutz	Wilfried Bohnert	~~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
Predictive Analytics	Prof. Dr. I. Keller	X	X	X	X	X	
Datensicherheit in der vernetzten Welt	Prof. Dr. I. Keller	X	X	X	X	X	
Penetration Testing	Wilhelm Dolle	X	X		X	X	
Cloud Security	Johann Loran	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. Podebrad	X	X		X	X	
OT-Sicherheit	Dan-Marvin Gluba, Lars Schmidt	X		X	X		X
Sicherheit im BOS-Umfeld	Prof. Dr. Walter Gora	X		X		X	X
Informationssicherheits-Managementsysteme (ISMS)	Sebastian Reinhardt	X		X	X	X	
Sicherheitstechnische Untersuchungen kritischer Infrastrukturen (KRITIS)	Prof. Dr.-Ing. habil. Manfred Mertins	X		X			X
Risikoanalyse und Risikomanagement	Carsten Baeck	X		X		X	X
Business Continuity Management (BCM)	Robert Osten, Dan Gluba	X	X	X	X	X	X
Social Engineering	Prof. Dr. S. Humer	X		X		X	X
Personenschutz	Wilfried Bohnert			X		X	X

1. **Predictive Analytics**

Modul-Nr./Code:	SM2088
WPM-Bezeichnung:	Predictive Analytics
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	• SecMan Master, 1./2./3. Semester, WPM • Wirtschaftsinformatik-Master als Teil des WPMs „Predictive Analytics and Privacy“
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Informationssicherheit • IT-Forensik • Business Continuity und Krisen-Management • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller, Dipl.-Math. David Fuhr
Lehrsprache:	Deutsch und ggf. Englisch
Voraussetzungen:	Grundlagen der Statistik, Data Warehousing, XML/HTML, möglichst 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 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 Kompetenzen zur Modellierung und Simulation von Prozessdaten und Benutzerverhalten. 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, der IT-Sicherheit, dem Operations Management und der Betrugserkennung ab.

Inhalte:	Den Studierenden werden hierbei Kenntnisse zu folgenden grundlegenden Themenbereichen vermittelt: • Aufbereitung nicht-numerischer Daten aus heterogenen Quellen (Big Data), • Maschinelles Lernen, Clusterung und Visualisierung, Predictive Modelling, Deep Learning
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• 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. **Datensicherheit in der vernetzten** Welt

Modul-Nr./Code:	SM2093
WPM-Bezeichnung:	Datensicherheit in der vernetzten Welt
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	• SecMan Master, 1./2./3. Semester, WPM • Wirtschaftsinformatik Master als Teil des WPMs „Predictive Analytics and Privacy“
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Informationssicherheit • IT-Forensik • Business Continuity und Krisen-Management • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller, Dipl.-Math. David Fuhr
Lehrsprache:	Deutsch
Voraussetzungen:	Grundlagen des Datenschutzes, Risikomanagement, möglichst Predictive Analytics
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 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:	Das Ziel dieser Lehrveranstaltung ist es, die IT- und Informations-Sicherheitsaspekte vernetzter Dienste aus Effizienz-Sicht zu betrachten. Ziel sind Pareto-Prinzipien, bei minimaler Datenbasis das Gros der Qualität, bzw. Resilienz zu behalten. Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden eine grundsätzliche Sensibilisierung für eine nachhaltige unternehmerische Governance. Damit werden sie in die Lage versetzt, moderne Technologien wie Big Data und Data Mining/Predictive Analytics effektiv und im Einklang mit ethischen und normenrechtlichen Anforderungen der Informationssicherheit auszuwählen und einzusetzen. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz.
Inhalte:	Den Studierenden werden hierbei zu folgenden Themen Informationen vermittelt: • Risikoappetit und Monte Carlo-Simulation mit Excel • Datenverarbeitung mit komfortablen KI-Bibliotheken und Tools • Process Mining zum Erreichen einer hohen Resilienz • Nachhaltige Compliance, serviceorientierte Organisation und Datensouveränität, technische Umsetzung von 80-/20-Prinzipien
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Gudehus, T.: Logistik – Grundlagen - Statistik - Anwendungen, Springer,4. Aufl., 2010 • Helisch, M.: Security Awareness, <kes>, 2009 • Logemann, T., „Datenschutz in Unternehmen“, 2016 • Zuboff, S.: „Überwachungskapitalismus“, 2018 Weitere Literatur wird in der Vorlesung bekannt gegeben.
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: • 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 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:	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. Gleichermaßen 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:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Kenntnisse über potenzielle Cyber-Risiken • Angreifertypen: Von Script Kiddies bis Advanced Persistant 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:	• 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

Modul-Nr./Code:	SM2021
Modulbezeichnung:	Cloud Security
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: • 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:	Grundlegende Kenntnisse und Verständnis von IT-Systemarchitekturen, Softwarearchitekturen, Secure Development Lifecycle und Cloud Computing. Technische Kenntnisse von Betrieb und dem Absichern von Cloud-Plattformen sind empfehlenswert, ebenso Programmierkenntnisse in Python, JSON und YAML.
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 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 Wahlpflichtmoduls besitzen die Studierenden Kenntnisse, um Cloud-Umgebungen und Cloud-Anwendungen zu verstehen sowie diese mit Hilfe von Sicherheitsprinzipien und -Konzepten zu analysieren. Risiken und Bedrohungen können verstanden, bewertet und geeignete Maßnahmen zur deren Absicherung ergriffen werden.
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Sichere Cloud-Architekturen und -Konzepte • Rechts- und Compliance-Grundlagen • Cloud-Daten-, Plattform- und Infrastruktursicherheit • Anwendungssicherheit in der Cloud • Sicherer Betrieb von Cloud-Umgebungen
Lehr- und Lernmethoden:	Interaktiver Mix aus Vorlesung, Übungen in Kleingruppen und praktischen Übungen.
Literatur:	• 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.
Besonderes:	//

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: • 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
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:	• Data Center: Richtlinien und normative Hintergründe • Risikoanalyse und Risikobewertung • Data Center Designs/Redesigns • Auswirkung organisatorischer, technischer, physischer und logischer IT-Sicherheit • Planung, Konzeption und Dimensionierung hinsichtlich: o Lage und Gebäude o Leistungs- und Platzbedarf o Zutrittsschutz und Einbruchschutz o Aktiver und passiver Brandschutz o Stromversorgung o Regelung der Umgebungsbedingungen o Kommunikations-Verkabelung o Redundanzkonzepte o Effizienz • Zuverlässigkeit, Verfügbarkeit, Fehlertoleranz, Resilienz • Nachhaltiger Betrieb und KPI‘s • Qualitative und quantitativer Verfahren zur Zertifizierung
Lehr- und Lernmethoden:	• Vorlesung/Vorträge mit wechselnden Medien • Workshops in Kleingruppen • Geführte Inspektion von Data Centern
Literatur:	• 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: • 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 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: • 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:	• Vorlesung/ Vorträge mit wechselnden Medien (Beamer, Flipchart, Whiteboard) • Übungen in Kleingruppen und zusammen.
Literatur:	• 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 • Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann, Dieter Wöhrle: Naturwissenschaft - Rüstung - Frieden: Basiswissen für die Friedensforschung, VS-Verlag, 2007 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
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: • 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:	Klausur oder Hausarbeit. Die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	Lt. SPO
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Faktenwissen zu populären Kryptographie-Lösungen • Beurteilen erfolgskritischer Fragen beim praktischen Einsatz von Kryptographie • Die Fähigkeit, sichere von unsicheren Kryptographieanwendungen zu unterscheiden • Verständnis für die Herausforderungen beim Einsatz moderner Kryptographie

Inhalte:	Das Modul konzentriert sich auf Fragestellungen der *Anwendung* bereits bewährter Kryptographieprotokolle (wie SSL/TLS); die mathematisch-technischen Grundlagen dieser werden nicht weiter vertieft. Das Wissen wird anhand von Beispielen erarbeitet, die den Studierenden aus dem alltäglichen Umgang mit Computern bereits bekannt sind. Diese beinhalten: • Best Practices der PKI am Beispiel von Transport Layer Security (SSL/TLS) • Realisierung von Diensten in der Cloud, die auch bei Kompromittierung des Cloudbetreibers ihre Integriät und Vertraulichkeit nicht verlieren am Beispiel von TOR, Signal Messenger und Blockchain • Architekturmerkmale sicherer Kommunikationsdienste am Beispiel von Online-Messengern • Ermöglichen eines sicheren Applikationsdesigns durch den Einsatz von Kryptographie am Beispiel von Passwortsafes • Nutzen und Herausforderung von Kryptographie in Hardware am Beispiel von Hardware Security Modules (HSM) und Trusted Plattform Modules (TPM) • Gewährleistung von Manipulationssicherheit am Beispiel von Wahlcomputern
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen, Vorstellung von Praxisbeispielen, technische Übungen am eigenen Laptop
Literatur:	• 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:	

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: • 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
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:
	
	• Datenträgeranalyse
	  • 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. 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
	  • 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
	  • Grundlagen
	  • Protokolle
	  • Detail-Analyse
	  • Anomalien
	  • verdeckte Kommunikation
	  • Angriffstypen

Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.

Literatur:	• 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:	<Modul Nr>
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: • 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:	M.A. Dan-Marvin Gluba
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
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: • 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:	• NIST SP 800 series • ISO/IEC 62443 • Bundesamt für Sicherheit in der Informationstechnik, ICS-Security-Kompendium (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.), Cyber-security of SCADA and Other Industrial Control Systems, Advances in Information Security Band 66 (Juni 2018).
Besonderes:	//

10. Sicherheit im BOS-Umfeld

Modul-Nr./Code:	SM2005
Modulbezeichnung:	Sicherheit im BOS-Umfeld
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: • 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:	Prof. Dr. Walter Gora, Philipp Ahlers
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: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Mündliche Prüfung/Präsentation und/oder Hausarbeit
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach dem Modul können die Studierenden die verschiedenen Anforderungen an die IT-Sicherheit in Behörden und Organisationen mit Sicherheitsaufgaben und deren Arbeitsweise verstehen. Sie können vorhandene und zukünftige Organisations- und IT- Strukturen analysieren; diese bezüglich Sicherheitsanforderungen bewerten und kennen die gesetzliche Rahmenbedingungen. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz.

Inhalte:	Den Studierenden werden vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Wer sind die BOS? Grundlagen, Struktur, Aufgaben, Verantwortlichkeiten und Rahmenbedingungen • Die Sicherheitsarchitektur in Deutschland – Anforderungen, Beteiligte, Rollen, Kompetenze und Zuständigkeiten • Aktuelle Herausforderungen und Projekte im Bereich der Informations- und Kommunikationstechnik bei der Polizei • Beispiel: Digitalfunk BOS als gemeinsame Infrastruktur: Historie, Entwicklung, aktueller Stand und Weiterentwicklung • Zentralstellenfunktion des BKA und gesetzliche Grundlagen (BKA-Gesetz) • Föderale Aufteilung: Länderhoheiten und -kompetenzen, Rolle kommunaler Organisatione • Europäische Einbindung und Vernetzung (Schengen/SIS, VIS, Eurodac, Europol, Frontex u a.) • Zusammenarbeit mit den Diensten (polizeilicher Staatsschutz, Nachrichtendienst etc.) • Die IT-Landschaft der Polizei – Übersicht, Besonderheiten und Kooperationsgemeinschafte • Digitalisierung polizeilicher Prozesse, Smart Policing • Übersicht zu typischen Anwendungen der Polizeien (Vorgangsbearbeitung, Fahndung, Fallbearbeitung, Ermittlungsunterstützung, Leitstellen, Telekommunikationsüberwachung etc.) • Fallbeispiel: Telekommunikationsüberwachung (TKÜ) • Die Rolle der Privatwirtschaft
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	Empfohlene Literatur: • Bäcker, M. et al: „Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz“, C.H. Beck, München, 2018 • Honekamp, W., Povalej, R. (Hrsg.): „Polizei-Informatik 2017“, Tagungsband - Polizeiakademie Niedersachsen, Rediroma Verlag, April 2017 Ergänzende Literatur: • Möllers, M. (Hrsg.): „Wörterbuch der Polizei“, C.H. Beck, München, 3. Auflage, 2018 • Zur Thematik IT-Sicherheit: www.bsi.de Empfohlene Web-Seiten (keine Gewähr für den Inhalt dieser Seiten!) • https://www.polizei.de • https://www.bka.de/DE/AktuelleInformationen/Publikationen/BKA-Herbsttagungen/2016/ProgrammUndRedebeitraege/programmUndRedebeitraege_node.ht - siehe auch diverse Downloads der Redebeiträge/Vorträge • https://www.bka.de/DE/AktuelleInformationen/Publikationen/BKA-Herbsttagungen/2017/ProgrammUndRedebeitraege/programmUndRedebeitraege_node.ht - siehe auch diverse Downloads der Redebeiträge/Vorträge • Diverse Seiten bei https://verfassungsblog.de, z. B.: https://verfassungsblog.de/im-netz-der-sicherheit-das-bka-gesetz-und-die-grenzen-der-zentralisierung/ • https://police-it.org/ (Hinweis: Meist tendenziöse, aber inhaltlich durchaus fundierte Artike • https://www.unibw.de/inf/studium/studiengang-cyber-sicherheit
Besonderes:	//

11. 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: • 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
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 eigenständige ISMS-Konzept zu erstellen. Die erworbenen fachlichen und methodischen Kompetenzen zielen auf die Vorbereitung für das Berufsleben ab.

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • ISO 27001 und ff. • BSI IT-Grundschutz • Unterschiede und Gemeinsamkeiten • Erfolgsfaktoren bei der Umsetzung
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• BSI-Standard 100-1: Managementsysteme für Informations-sicherheit (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:	//

12. Sicherheitstechnische Begutachtung kritischer Infrastrukturen (KRITIS)

Modul-Nr./Code:	SM2089
Modulbezeichnung:	KRITIS - Anforderungen an die Auslegung, den Betrieb und die sicherheitstechnische Untersuchung kritischer Infrastrukturen
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: • Informationssicherheit • Business Continuity und Krisen-Management • 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 oder 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 Auslegung von Kernkraftwerken (KKW) zu berücksichtigende Stör- und Unfälle vermittelt. Dafür werden Methoden zur Bewertung von Gefährdungen kritischer Infrastrukturen infolge naturbedingter oder zivilisationsbedingter Einwirkungen vorgestellt und eine Übersicht über Sicherheitskonzepte für KKW mit Bedeutung für Konzepte zum Schutz kritischer Infrastrukturen, Schwerpunkt „Gestaffeltes Sicherheitskonzept“ gegeben. Die

	Studierenden werden Prüfkonzepten zur Sicherstellung und zum Erhalt erforderlicher Qualitätsmerkmale bei Fertigung, Errichtung und Betrieb von KKW einschließlich 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 auf den Gebieten von Strahlenschutz und nuklearer Sicherheit wird vorgestellt. Die Bewertung von Bedrohungen aus einer globalisierten Welt für die Integrität kritischer Infrastrukturen wird diskutiert. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz.
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Analyse von Stör- und Unfällen mit Bedeutung für kritische Infrastrukturen, insbesondere für KKW • Anwendung deterministischer und probabilistischer Analysemethoden zur Bewertung der sicherheitstechnischen Bedeutung von Betriebserfahrungen sowie neuen Erkenntnissen für die Integrität und Funktionsweise kritischer Infrastrukturen, einschließlich KKW • Konzepte zum Schutz von KKW 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 • Zuständigkeiten für Genehmigung und Aufsicht von KKW • 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:	• 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. • Laufs: Reaktorsicherheit für Leistungskernkraftwerke, Springerverlag 2013.
Besonderes:	//

13. 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: • 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 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 ve sowie deren Ergebnisse einzuschätzen und anzuwenden. Sie beherrschen die theoretischen
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt: • Verschiedene Ansätze der Risikoanalyse • Probabilistische und deterministische Ansätze • Retrospektive und prospektive Analysen • Qualitative und quantitative Ansätze • Umgang mit Unsicherheiten

	• Ansätze aus dem Qualitätsmanagement, bzw. der Sicherheitsbewertung technischer Sys • Management von Risiken in verschiedenen Umgebungen • Etablierte Frameworks des Risikomanagements
Lehr- und Lernmethoden:	• Vorlesung/ Vorträge mit wechselnden Medien (Beamer, Flipchart, Whiteboard) • Übungen in Kleingruppen und zusammen
Literatur:	• British Standard - 25999: Business Continuity Management [Buch], London, 2006 • Brühwiler Bruno - Risikomanagement als Führungsaufgabe: ISO 31000 mit ONR 49000 • Brühwiler Bruno und Romeike Frank - Strategische Früherkennung [Buch], 2010 • http://www.controllingwiki.com/de/index.php/Risikoanalyse_FMEA. • Dornes Nadeshda - Alternative Risikomodellierungs-, Risikoanalyse- und Bewertungsme • eurorisk.ch [Online], http://www.eurorisk.ch/.fh-hannover.de, 2015 http://transfer.tr.fh • http://www.es.hsmannheim.de/sps/Uebungen/Kapitel8/Uebung8_2.html • maschinenrichtlinie-2006-42-eg.de [Online], 2015, http://www.maschinenrichtlinie-2006 • ONR 49000, 2010 • ONR 49002-1, 2010 • ONR 49002-2, 2010 • orghandbuch.de [Online], 2015 http://www.orghandbuch.de/OHB/DE/Organisationshandbuch/6_MethodenTechniken/6 • pwc.de [Online], 2015, http://www.pwc.de/de/risiko-management/studie-offenbart-ma • risikomanager.org [Online], 2015, http://risikomanager.org/methodenassistent/fehlerbaumanalyse/.risknet.de [Online], 2 • Romeike Frank und Hager Peter - Erfolgsfaktor Risiko-Management 3.0: Methoden, Beis
Besonderes:	//

14. 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: • 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:	Den Studierenden werden vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • 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:	• 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:	//

15. 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: • 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. 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 oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach dem Modul können die Studierenden verschiedene Ansätze von Social Engineering analysieren und verstehen. Den Studierenden werden Möglichkeiten und Grenzen der sozialen Manipulation in digitalen Umgebungen aufgezeigt. Die Lernenden erwerben die Fähigkeit, Social Engineering in ganz unterschiedlichen Fallbeispielen selbständig zu erkennen und Abwehrmethoden zu entwickeln. Dabei geht es sowohl um allgemeingesellschaftliche Gestaltung, als auch um anwendungsorientierte Fälle. Sie beherrschen die

	theoretischen Grundlagen, um diese kognitiv, intuitiv und kreativ in der Studienarbeit umzusetzen.
Inhalte:	Den Studierenden werden zu folgenden Themen Informationen vermittelt: Social Engineering sowohl als „Gesellschaftsgestaltung“, als auch im „kleinen Fall“, d.h. in Form eines Angriffs auf digitale Firmeninfrastruktur via Menschen (d.h. Mitarbeiter, Externe, Partner, etc.)
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Baumann, U., Schimmer, K., Fendl, A. (Hg.): SAP Pocketseminar: Faktor Mensch. Die Kunst des Hackens oder warum Firewalls nichts nützen. SAP 2005 (PDF) • Conheady, S.: Social Engineering in IT Security: Tools, Tactics and Techniques. McGraw-Hill Education, 2014 • Duff, A.: Social Engineering in the Information Age. The Information Society, 21: 67-71, 2005 • Ekman, P. & Hadnagy, C.: Social Engineering enttarnt: Sicherheitsrisiko Mensch. mitp Professional, 2014 • Lardschneider, M.: Social Engineering. Datenschutz und Datensicherheit – DuD. 09/2008, 32/9, S. 574-578 • Schumacher, S.: Psychologische Grundlagen des Social Engineering. Datenschleuder 94/2010, S. 52-59. Siehe dazu auch: Schumacher, S.: Die psychologischen Grundlagen des Social Engineerings. Magdeburger Journal zur Sicherheitsforschung, Bd. 1, 2011, S. 1–26
Besonderes:	//

16. Personenschutz

Modul-Nr./Code:	SM2071
Modulbezeichnung:	Personenschutz
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: • 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:	Wilfried Bohnert
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:	Praktische Arbeit + mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Bei Abschluss des Lernprozesses werden die Studierenden in der Lage sein, ein Sicherheitskonzept zum Schutze von Personen („gefährdete Person und Familienangehörige“) zu erstellen und den Aufbau, die Umsetzung und die Steuerung von Personenschutz-Gruppen in der täglichen Praxis durchführen können. Sie kennen die Methoden der Schutz- und Sicherheitstechnik und analysieren die Einsatzmöglichkeiten mechanischer und elektronischer Sicherheitseinrichtungen in Anwesen von VIPs. Nach erfolgreichem Abschluss des Moduls besitzen die Studierenden auch Kenntnisse über Travel Risk Management, Veranstaltungsschutz, Bedrohungen von Unternehmen, Räumung von Gebäuden im Zusammenhang mit Bedrohungen, Sozial Engineering und dem Aufbau und der Steuerung von Lagezentren.
Inhalte:	1. Gefährdungsanalyse 1.1 Einstufung durch LKÄs

	1.2 Betreuung der Familie (Ehefrau, Kinder, usw.) 1.3 Sicherheits-Konzept bei Angehörigen von Unternehmen mit steuerlichen Hinweisen 2. Entwicklung von Schutzzielen 3. Ablaufdiagramm Personenschutz 4. Auswahl von Personenschutzdienstleistern 5. Methodisch-theoretischer Teil: Festlegung/Umsetzung der Maßnahmen, Veränderung beim Nachlassen der körperlichen Leistungsfähigkeit 6. Praxis des Strafrechts: Strafprozessrecht, Notwehr/Nothilfe, Notstand, Waffenrecht, Waffentechnik, Terrorismus, Aufklärung/Observation, Sportausbildung, Schießausbildung, Fahrausbildung, Erste Hilfe, Durchsuchung von Räumen und Kfz., Verhalten bei Auffinden von subversiven Gegenständen, Funkunterweisung 7. Randbereiche 7.1 Travel Risk Management 7.2 Veranstaltungsschutz (z. B. Hauptversammlungen) 7.3 Bedrohungen von Unternehmen („Bombendrohung“) 7.4 Räumung im Zusammenhang mit „Bomben-drohungen“ 7.5 Sozial Engineering 7.6 Lagezentrum (Zusammenspiel bei z. B. Erpressung)
Lehr- und Lernmethoden:	Vorlesung, Bearbeitung von Fallbeispielen in Kleingruppen, Vorstellung von Praxisbeispielen, Rollenspiele
Literatur:	• Richard Boorberg Verlag Stuttgart: Personenschutz 2003 (Arbeitshandbuch) • Sicherheitsberater: Nummer 5, 01.03.2017 „Schwerpunkt Veranstaltungsschutz • MediaSec AG, Forch/Zürich – Sicherheitsforum: Planungshandbuch Videoüberwachungsanlagen
Besonderes:	//