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: September 2018

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:	September 2018

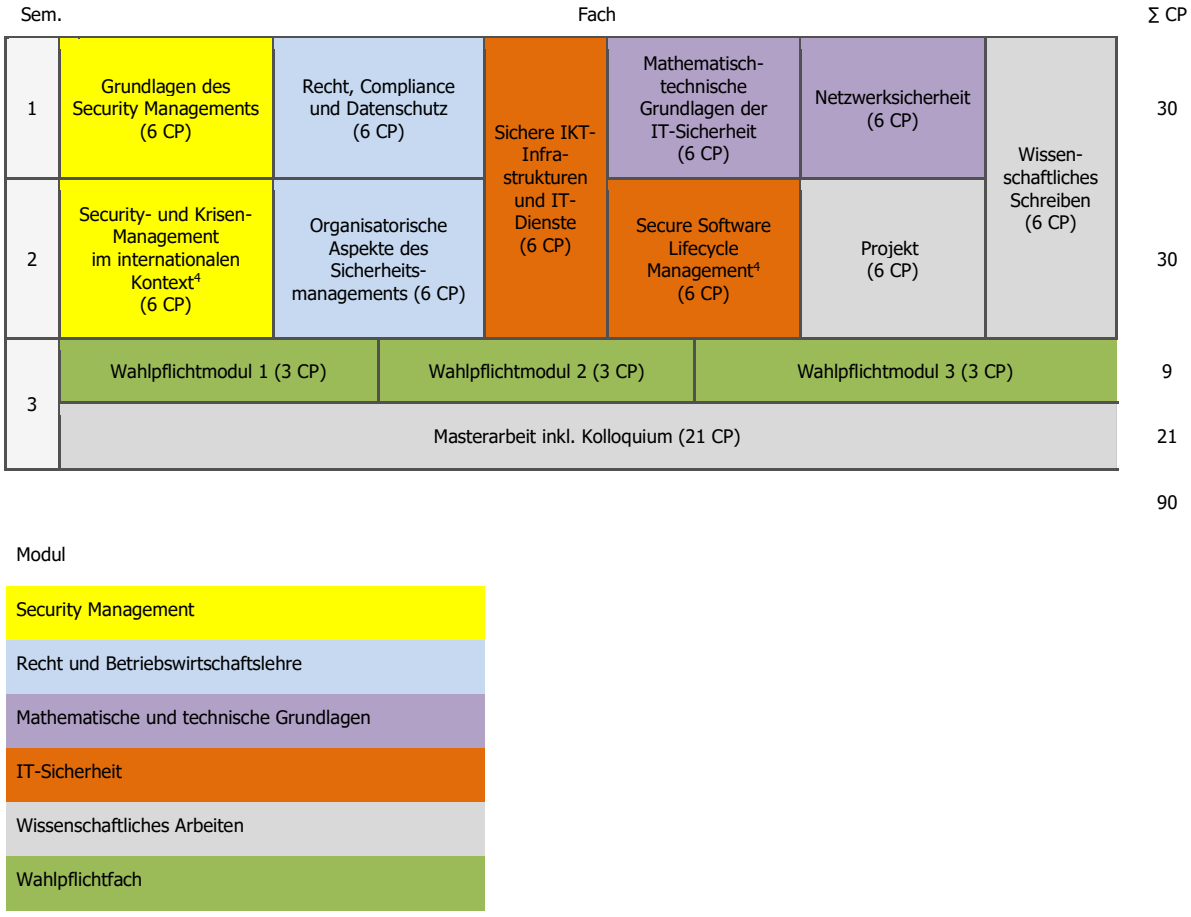
Inhaltsverzeichnis

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 Fachübersicht des Studiengangs Security Management



[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] *SecMan im int. Kontext* und *SSLM* sind Pflichtfächer für Wirtschaftsinformatik (M.Sc.)

Angebotene Wahlpflichtmodule und Profilrichtungen

Im jedem Semester werden mindestens 1 bis 2, in der Regel 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 2016	WiSe 16/17	SoSe 2017	WiSe 17/18	SoSe 2018	WiSe 18/19	SoSe 2019
Predictive Analytics	Prof. Dr. Ivo Keller	X		X		X		X
Datensicherheit in der vernetzten Welt	Prof. Dr. Ivo Keller	X		X		X		X
Penetration Testing	Wilhelm Dolle	X		X		X		X
Secure Data Center (ehem. Sicherheit von Rechenzentren)	Uwe Müller	X		X		X		X
Cyber Security	Ingo Ruhmann	X		X		X		X
Sicherheit im BOS-Umfeld	Prof. Dr. Walter Gora						X	
Payment Card Industry Data Security Standard (PCI DSS)	Patrick Sauer				X			
Informationssicherheits-Managementsysteme (ISMS)	Tobias Goldschmidt		X		X		X	
Sicherheitstechnische Begutachtung kritischer Infrastrukturen (KRITIS)	Prof. Dr. habil. Manfred Mertins		X		X		X	
Technische Aspekte der IT-Forensik	Prof. Dr. Igor Podebrad	X			X		X	
Risikoanalyse und Risikomanagement	Carsten Baeck		X		X		X	
Social Engineering	Prof. Dr. Stephan Humer		X		X		X	
Business Continuity Management (BCM)	Prof. Dr. Oliver Weissmann	X			X		X	
IT Infrastructure Library (ITIL)	Prof. Dr. Jochen Scheeg	X		X				
Personenschutz	Gerhard Reinhardt						X	

Tabelle 2: Zuordnung der WPM zu den Vertiefungsrichtungen

Kursname	Dozent	Informationssicherheit	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	
Datensicherheit in der vernetzten Welt	Prof. Dr. I. Keller	X	X	X	X	X	
Penetration Testing	Wilhelm Dolle	X	X		X	X	
Secure Data Center	Uwe Müller	X	X	X	X	X	X
Cyber Security	Ingo Ruhmann	X	X	X	X	X	
Sicherheit im BOS-Umfeld	Prof. Dr. Walter Gora	X	X	X	X		X
Payment Card Industry Data Security Standard (PCI DSS)	Patrick Sauer	X	X		X	X	
Informationssicherheits-Managementsysteme (ISMS)	Tobias Goldschmidt,	X	X	X	X	X	
Sicherheitstechnische Untersuchungen kritischer Infrastrukturen (KIRITS)	Prof. Dr.-Ing. habil. Manfred Mertins	X		X			X
Technische Aspekte der IT-Forensik	Prof. Dr. I. Podebrad	X	X	X	X	X	
Risikoanalyse und Risikomanagement	Carsten Baeck	X	X	X	X	X	X
Social Engineering	Prof. Dr. S. Humer	X	X	X	X	X	X
IT Infrastructure Library (ITIL)	Prof. Dr. J. Scheeg	X	X	X	X	X	X
Business Continuity Management (BCM)	Prof. Dr. O. Weissmann	X	X	X	X	X	X
Personenschutz	Gerhard Reinhardt			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 • Forensik • IT und Cyber Security • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller
Lehrsprache:	Deutsch und Englisch
Voraussetzungen:	Grundlagen der Statistik, Data Warehousing, XML/HTML
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 im Umgang mit Methoden zur Verarbeitung von Prozessdaten, Benutzerverhalten und Meinungen. Sie verwenden dafür Visualisierungstools (z. B. Rapid Miner, Matlab, Python). Die erworbenen fachlichen und methodischen Kompetenzen zielen auf die Vorbereitung für das Berufsleben 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:	• Anasse B., „Predictive Analytics for Dummies", John Wiley & Sons, 2014 • Duda, R. O., Hart, P. E., Stork D. G., "Pattern Classification", 2nd edition, John Wiley & Sons, New York, 2001 • Haberich, R., „Future Digital Business", 2013 • Keller, I., „Klassifikation in der Multimedia-Kommunikation", Vorlesungsscript an der TU Berlin, Stand Juli 2014 • http://docs.rapidminer.com/downloads/RapidMiner-v6-user-manual.pdf, Stand 2018
Besonderes:	//

Module no./code:	SM2088
Module description:	**Predictive analytics**
Division into teaching sessions, if applicable:	//
Duration of module:	One semester
Classification in the curriculum:	• SecMan master, 1st/2nd/3rd semester, WPM • Business informatics master as part of WPMs "Predictive analytics and privacy"
Usability of the module:	This module can be used for the following profile specialisms: • Information security • Forensic science • IT and cyber security • Bank security
Frequency offered:	Every academic year
Module leader:	Prof. Dr. Ivo Keller
Lecturer:	Prof. Dr. Ivo Keller
Language of instruction:	German and English
Prerequisites:	Principles of statistics, data warehousing, XML/HTML
ECTS credits:	3
Total workload and composition of course:	90 hrs. = 30 hrs. attendance and 60 hrs. self-study (incl. examination preparations and examination)
Form of teaching/semester hours per week:	Lectures: 30 hours
Study and examination requirements:	Homework or presentation / oral examination; the exact form of examination will be announced at the beginning of the semester.
Weighting of the grade in the overall grade:	According to the study and examination regulations
Learning outcomes:	Upon successful completion of this module, students will have skills in dealing with methods for processing process data, user behaviour and opinions. They will use visualisation tools for this purpose (e.g. Rapid Miner, Matlab, Python). The acquired professional and methodical competences are geared toward preparation for professional life.

Contents:	The students are taught knowledge from the following basic topics: • Processing non-numerical data from heterogeneous sources (big data), • Machine learning, clustering and visualisation Predictive modelling, deep learning
Teaching and learning methods:	Lectures, workshops in small groups.
Literature:	• Anasse B., "Predictive Analytics for Dummies", John Wiley & Sons, 2014 • Duda, R. O., Hart, P. E., Stork D. G., "Pattern Classification", 2nd edition, John Wiley & Sons, New York, 2001 • Haberich, R., "Future Digital Business", 2013 • Keller, I., "Klassifikation in der Multimedia-Kommunikation", lecture script from TU Berlin, dated July 2014 http://docs.rapidminer.com/downloads/RapidMiner-v6-user-manual.pdf, dated 2018
Additional information:	//

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 • 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
Lehrsprache:	Deutsch und Englisch
Voraussetzungen:	Grundlagen des Datenschutzes, 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-Sicherheits- und Datenschutzaspekte vernetzter Dienste aus Sicht des Data Minings zu betrachten. Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden eine grundsätzliche Sensibilisierung für eine nachhaltige unternehmerische Governance. Damit sollen die Studierenden in die Lage versetzt werden, moderne Technologien wie Big Data und Data Mining/Predictive Analytics sicher und im Einklang mit ethischen und normenrechtlichen Anforderungen des Daten- und Persönlichkeitsschutzes auszuwählen und einzusetzen. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz.
Inhalte:	Den Studierenden werden hierbei zu folgenden Themen Informationen vermittelt: • Tools zur Textindexierung (z. B. Solr/Lucene) • Verantwortung der Datenverarbeitung gegenüber den Quellen, Persönlichkeitsschutz als Grundrecht • Datensicherheit als Voraussetzung für unternehmerische Existenz • Nachhaltige Compliance, serviceorientierte Organisation und Datensouveränität, technische Umsetzung von 80-/20-Prinzipien
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Witt, B.C., Datenschutz kompakt • Helisch, M.: Security Awareness, <kes>, 2009 • Logemann, T., „Datenschutz in Unternehmen" • Hofstetter, Y., „Das Ende der Demokratie", Bertelsmann, 2016 Weitere Literatur wird in der Vorlesung bekannt gegeben.
Besonderes:	//

Module no./code:	SM2093
Module description:	**Data security in the networked world**
Division into teaching sessions, if applicable:	//
Duration of module:	One semester
Classification in the curriculum:	• SecMan master, 1st/2nd/3rd semester, WPM • Business informatics Master as part of WPMs "Predictive analytics and privacy"
Usability of the module:	This module can be used for the following profile specialisms: • Information security • Forensic science • Business continuity and crisis management • IT and cyber security • Bank security
Frequency offered:	Every academic year
Module leader:	Prof. Dr. Ivo Keller
Lecturer:	Prof. Dr. Ivo Keller
Language of instruction:	German and English
Prerequisites:	Principles of data protection, possibly predictive analytics
ECTS credits:	3
Total workload and composition of course:	90 hrs. = 30 hrs. attendance and 60 hrs. self-study (incl. examination preparations and examination)
Form of teaching/semester hours per week:	Lectures: 30 hours
Study and examination requirements:	Homework or presentation / oral examination; the exact form of examination will be announced at the beginning of the semester.
Weighting of the grade in the overall grade:	According to the study and examination regulations

Learning outcomes:	The goal of this course is to examine IT security and privacy aspects of networked services from a data mining perspective. After successfully completing this module, the students will have a basic awareness of sustainable corporate governance. The aim is to enable students to select and use modern technologies such as big data and data mining / predictive analytics safely and in compliance with ethical and standard legal requirements of data and personal protection. The students will develop pronounced problem-solving and assessment competence.
Contents:	The students are given information on the following topics: • Text Indexing Tools (e.g. Solr/Lucene) • Responsibility of the data processing with respect to sources, protection of personality as a fundamental right • Data security as a prerequisite for entrepreneurial existence • Sustainable compliance, service-oriented organisation and data sovereignty, technical implementation of 80/20 principles
Teaching and learning methods:	Lectures, workshops in small groups.
Literature:	• Witt, B.C., Datenschutz kompakt • Helisch, M.: Security Awareness, <kes>, 2009 • Logemann, T., "Datenschutz in Unternehmen" • Hofstetter, Y., "Das Ende der Demokratie", Bertelsmann, 2016 Additional literature will be announced during the lectures.
Additional information:	//

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 • 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. 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 • Forensik • Business Continuity und Krisen-Management • IT und Cyber Security • 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 gesetzlichen 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, Kompetenzen 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 Organisationen • 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 Kooperationsgemeinschaften • 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.html - siehe auch diverse Downloads der Redebeiträge/Vorträge • https://www.bka.de/DE/AktuelleInformationen/Publikationen/BKA-Herbsttagungen/2017/ProgrammUndRedebeitraege/progra

	mmUndRedebeitraege_node.html - 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 Artikel) • https://www.unibw.de/inf/studium/studiengang-cyber-sicherheit
Besonderes:	//

5. Payment Card Industry Data Security Standard (PCI DSS)

Modul-Nr./Code:	SM2082
Modulbezeichnung:	**Payment Card Industry Data Security Standard (PCI DSS)**
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 • Forensik • IT- und Cybersecurity • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Patrick Sauer, 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 verstehen die Studierenden den PCI-DSS Standard im Detail. Sie werden in die Lage versetzt, mit ihren Kenntnissen und Fertigkeiten die Sicherheitsanforderungen an Webshops und Portale, welche Finanztransaktionen durchführen zu analysieren, zu bewerten und entsprechende Security und Datensicherheits- Maßnahmen vorzuschlagen. 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: • Sicherheitsanforderungen der Kreditkartenfirmen • Technische Umsetzungsmöglichkeiten • Zertifizierungsprozess
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Payment Card Industry Data Security Standard 3.2, PCI Council, 2016 • PCI DSS Made Easy: PCI DSS 3.2 Edition, Francois Desharnais und Yves B Desharnais, 2016 • PCI DSS 3.1: The Standard That Killed SSL, Branden R. Williams, 2015 • Information Technology Policies and Procedures for the Payment Card Industry Data Security Standard (PCI DSS), Thomas Miller, 2010 • PCI DSS - A Practical Guide to Implementing and Maintaining Compliance, Steve Wright, 2011 • Payment Card Industry Data Security Standard Handbook, Timothy M. Virtue, 2008
Besonderes:	//

6. 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 • Forensik • Business Continuity und Krisen-Management • IT- und Cybersecurity • Bankensicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Tobias Goldschmidt
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:	//

7. 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:	//

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 • Forensik • Business Continuity und Krisen-Management • 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. 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 • 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:
	  ○ 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 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.

10. 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 • 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:	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:	//

11. 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 • Forensik • Business Continuity und Krisen-Management • IT- und Cybersecurity • 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 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: • 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 Systeme • 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 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/risikowahrnehmung.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:	//

12. 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 • Forensik • Business Continuity und Krisen-Management • IT- und Cybersecurity • 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:	//

13. IT Infrastructure Library (ITIL)

Modul-Nr./Code:	SM2013
Modulbezeichnung:	**IT Infrastructure Library (ITIL)**
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 • 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. Jochen Scheeg
Dozent/in:	Prof. Dr. Jochen Scheeg
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/oder mündliche Prüfung und/oder Klausur und/oder Präsentation
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls sind die Studierenden in der Lage, das ITIL-Modells anzuwenden und Unternehmens- und Sicherheitsprozesse bezüglich der Umsetzung des ITIL-Modells zu bewerten. Die Studierenden sind mit den Grundlagen der Theorie und Praxis von ITIL (IT Infrastructure Library „v3") und IT Service Management vertraut. Ebenso besitzen sie Grundkenntnisse im Bereich des:

	• ITIL-Modells • 5 Phasen des ITIL-Lebenszyklus‘ o Service Strategy o Service Design o Service Transition o Service Operation und o Continual Service Improvement und ihre einzelnen Prozesse. Dies unterstützt die Studierenden bei der Suche nach Lösung im Entwicklungsprozess und bei der Generierung neuer Ideen. Ergänzend zur theoretischen Einführung werden verschiedene Praxisszenarien vorgestellt und praktisch erarbeitet. Es werden verschiedene Situationen von ITIL-Einführungen vorgestellt und die Bedeutung von ITIL an Beispielen durchgespielt. In Vorträgen werden einzelne Themen vertieft.
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt: Die Studierenden erhalten eine Einführung in ITIL (IT Infrastructure Library „v3“) und IT Service Management. Hierzu zählen: • ITIL-Modell • 5 Phasen des ITIL-Lebenszyklus‘ o Service Strategy o Service Design o Service Transition o Service Operation und o Continual Service Improvement und ihre einzelnen Prozesse. Ergänzend zur theoretischen Einführung werden verschiedene Praxisszenarien vorgestellt und praktisch erarbeitet. Es werden verschiedene Situationen von ITIL-Einführungen vorgestellt und die Bedeutung von ITIL an Beispielen durchgespielt. In Vorträgen werden einzelne Themen vertieft.
Lehr- und Lernmethoden:	• Vorlesung/Vorträge mit wechselnden Medien (Beamer, Flipchart, Whiteboard) • Übungen in Kleingruppen und zusammen.
Literatur:	• Jan van Bon, et al., Foundations in IT Service Management basierend auf ITIL v3, Van Haren Publishing, Zaltbommel 2008 • Jan van Bon, et al., Foundations in IT Service Management basierend auf ITIL, Zaltbommel 2006 • David Cannon, et al., ITIL Service Strategy 2011 Edition, TSO, London, 2011 • Lou Hunnebeck, et al., ITIL Service Design 2011 Edition, TSO, London, 2011 • Stuart Rance, et al., ITIL Service Transition 2011 Edition, TSO, London, 2011 • Randy Steinberg, et al. ITIL Service Operation 2011 Edition, TSO, London, 2011

	• Vernon Lloyd, et al., ITIL Continual Service Improvement 2011 Edition, TSO, London, 2011
Besonderes:	Im Anschluss an die Lehrveranstaltung ist es möglich, sich der Prüfung für das „ITIL Foundation"-Zertifikat zu unterziehen. Für diese Prüfung bestehen Sonderkonditionen bezüglich der Kosten.

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 • 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. Oliver Weissmann
Dozent/in:	Prof. Dr. Oliver Weissmann, Wolfgang Reibenspies
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. 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:	Gerhard Reinhardt
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:	//