Technische Hochschule
Brandenburg
University of
Applied Sciences

Technische Hochschule Brandenburg

Modulkatalog
des Masterstudiengangs
Security Management M.Sc.

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

1. Einleitung

Dieses Dokument beschreibt die Pflicht-Lehrgebiete[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].

Lehrgebietsübersicht (Regelstudienplan Vollzeit)

<table>
<tr><th>Sem</th><th colspan="6">Module</th><th>∑ CP</th></tr>
<tr><td>1</td><td>Grundlagen des Security Managements (6 CP)</td><td>Recht, Compliance und Datenschutz (6 CP)</td><td rowspan="2">Sichere IKT-Infra-strukturen und IT-Dienste (6 CP)</td><td>Mathematisch-technische Grundlagen der IT-Sicherheit (6 CP)</td><td>Netzwerksicherheit (6 CP)</td><td rowspan="2">Wissen-schaft-liches Schrei-ben (6 CP)</td><td>30</td></tr>
<tr><td>2</td><td>Security- und Krisenmanagement im internationalen Kontext[4] (6 CP)</td><td>Organisatorische Aspekte des Sicherheits-managements (6 CP)</td><td>Secure Software Lifecycle Management (6CP)</td><td>Projekt (6 CP)</td><td>30</td></tr>
<tr><td rowspan="2">3</td><td colspan="3">Wahlpflichtmodul 1 (3CP)</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="6"></td><td>90</td></tr>
</table>

Lehrgebiet

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

[1] Lehrgebiete 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.)

Lehrgebietsübersicht (Regelstudienplan Teilzeit)

Sem.	Module			
1	Grundlagen des Security Managements (6 CP)	Mathematisch-technische Grundlagen der IT-Sicherheit (6 CP)	Sichere IKT–Infrastrukturen und IT-Dienste (6 CP)	15
2	Security- und Krisenmanagement im internationalen Kontext (6 CP)	Organisatorische Aspekte des Sicherheitsmanagements (6 CP)		15
3	Netzwerksicherheit (6 CP)	Recht, Compliance und Datenschutz (6 CP)	Wissenschaftliches Schreiben (6CP)	15
4	Secure Software Lifecycle Management (6 CP)	Projekt (6CP		15
5	Wahlpflichtmodul 1 (3 CP)	Wahlpflichtmodul 2 (3 CP)		6
	Masterarbeit incl. Kolloquium (21 CP)			
6	Wahlpflichtmodul 3 (3 CP)			24
				90

Lehrgebiet

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

2. Grundlagen des Security Managements

Modul-Nr./Code:	SM110
Modulbezeichnung:	**Grundlagen des Security Managements**
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	Das Modul wird auch als Pflichtvorlesung des Master-Studiengangs Wirtschaftsinformatik angeboten. Das Modul kann auch für Master Informatik angeboten werden.
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Heinz-Dieter Schmelling
Dozent/in:	Prof. Dr. Heinz-Dieter Schmelling
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS:	Vorlesung: 30 Stunden (2 SWS), Praktische Anwendung und Übung an Fallbeispielen: 30 Stunden (2 SWS)
Studien-/Prüfungsleistungen:	Hausarbeit + Referat, alternativ mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden grundsätzliche Kenntnisse und Fertigkeiten zur Durchführung von Sicherheitsuntersuchungen und Risikobewertungen, Analyse von Sicherheitslagen und der Sinnhaftigkeit von Gegenmaßnahmen. Sie entwickeln ein Verständnis für die Bedeutung der Sicherheit als integralen Entscheidungsprozess im Unternehmern, können Sicherheitsorganisationen im Unternehmen beurteilen und haben beispielhaft Sicherheitsprozesse unter Zuhilfenahme von IT-Werkzeugen abgebildet, Sicherheitsmaßnahmen erarbeitet und trainiert, diese vor einem Entscheidungs-gremium erfolgreich durchzusetzen.

	Zusätzlich trainieren die Studierenden das Etablieren einer Sicherheitsorganisation in einem Unternehmen, die Erstellung eines Qualifikationsprofils für einen Sicherheitsverantwortlichen, die Integration von IT- und Nicht-IT-Sicherheits-relevanten Aspekten, die Einführung eines Sicherheitsmanagementsystems in einer Organisation und die Erarbeitung einer Strategie für einen Teilbereich der IT-, Informations- oder Unternehmenssicherheit. Sie beherrschen die theoretischen Grundlagen, um diese kognitiv, intuitiv und kreativ in der Studienarbeit umzusetzen.
Inhalte:	Wesentliche Aspekte der Unternehmenssicherheit: • Security Governance und Sicherheitsmanagementsystem • Security Organisation • Security Policy • Risikomanagement • Sicherheitsanalysen • Sicherheitsprozesse • Normen und Standards für Informationssicherheit • Return-on-Security-Investment-Berechnungen • Krisenmanagement • Business Continuity Management Zudem: • Ausgewählte Vertiefungsbereiche der IT- und der Unternehmenssicherheit
Lehr- und Lernmethoden:	Interaktiver Mix aus Vorlesung, Erarbeiten und Vortragen von Inhalten, Demonstration von Konzepten, praktischen Aufgaben in Gruppen, Erarbeiten von eigenen Inhalten und Rollenspiel.
Literatur:	• DIIR (Hrsg.): Handbuch Arbeits- und Unternehmenssicherheit in Kreditinstituten, 2012 (ISBN 978-3503138623) • Klaus-Rainer Müller: Handbuch Unternehmenssicherheit, Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System, 2015 (ISBN 978-3658101503) • Heinrich Kersten, Gerhard Klett: Der IT Security Manager: Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden, 2015 (978-3658099732) • Heinrich Kersten u. a.: IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, 2016 (978-3658146931) • Axel Bede: Notfall- und Krisenmanagement im Unternehmen, 2009 (ISBN 978-3938062869)
Besonderes:	//

3. Security- und Krisenmanagement im internationalen Kontext

Modul-Nr./Code:	SM120
Modulbezeichnung:	**Security- und Krisenmanagement im internationalen Kontext**
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	//
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Heinz-Dieter Schmelling
Dozent/in:	Prof. Dr. Heinz-Dieter Schmelling
Lehrsprache:	Deutsch und Englisch
Voraussetzungen:	//
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS:	Vorlesung: 30 Stunden (2 SWS), Übung: 30 Stunden (2 SWS)
Studien-/ Prüfungsleistungen:	Hausarbeit + Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach dem Modul können die Studierenden verschiedene Ansätze zur Analyse von Sicherheitslagen im internationalen Kontext unter Berücksichtigung kultureller, politischer und geographischer Gegebenheiten und über die Führung einer Sicherheitsorganisation in internationalen Konzernen verstehen und beurteilen. Sie erlangen Fähigkeiten zur Erarbeitung von Sicherheitsmaßnahmen bei Reisen oder der Entsendung von Mitarbeitern ins Ausland. Die Studierenden kennen die Einführung eines Krisenmanagements, die Reaktion in internationalen Krisensituationen und die Steuerung der globalen Krisenkommunikation sowie der öffentlichen Wahrnehmung von Sicherheitsthemen. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz auf den Gebieten:

Inhalte:	• Sicherheitsmanagement in globalen Organisationen • Travel Security • Sicherheit bei Entsendung von Mitarbeitern • Krisenmanagement im internationalen Umfeld • Krisenkommunikation: Prinzipien und Vorgehensweisen bei der Kommunikation in Krisenfällen • Interne und externe Krisenkommunikation • Message House • Umgang mit den Medien in Krisensituationen • Außenwirkung von Sicherheit • Kampagnen für Sicherheitsthemen
Lehr- und Lernmethoden:	Interaktiver Mix aus Vorlesung, Erarbeiten und Vortragen von Inhalten, Demonstration von Konzepten, praktischen Aufgaben in Gruppen, Erarbeiten von eigenen Inhalten und Rollenspiel.
Literatur:	• Leidel, Sven: Handbuch Reisesicherheit, 2014 (ISBN 978-3-735777256) • Ansgar Thießen (Hrsg.): Handbuch Krisenmanagement, 2014 (ISBN 978-3658042929) • Lorenz Steinke: Kommunizieren in der Krise, 2014 (ISBN 978-3658043667) • Stephan Gundel (Hrsg.): Sicherheit für Versammlungsstätten und Veranstaltungen: Ein umfassendes Handbuch zur Sicherheitskonzeption, 2017 (ISBN 978-3415059566) • Wei Ning Zechariah Wong: Business Continuity Management System: A Complete Guide for Implementing ISO 22301, 2014 (ISBN 978-0749469115) • Thomas, Alexander: Interkulturelle Handlungskompetenz, 2011 (978-3-834930156) • Garthwaite, Rosie: Handbuch für die gefährlichsten Orte der Welt, 2011 (978-3-827010360)
Besonderes:	//

Module no./code:	SM120
Module description:	**Security and crisis management in an international context**
Division into teaching sessions, if applicable:	//
Duration of module:	One semester
Classification in the curriculum:	Secman master, 2nd semester, core module
Usability of the module:	//
Frequency offered:	Every academic year
Module leader:	Prof. Dr. Heinz-Dieter Schmelling
Lecturer:	Prof. Dr. Heinz-Dieter Schmelling
Language of instruction:	German and English
Prerequisites:	//
ECTS credits:	6
Total workload and composition of course:	180 hrs. = 60 hrs. attendance, 120 hrs. self-study (incl. Examination preparation and examination)
Form of teaching/semester hours per week:	Lectures: 30 hours, workshops: 30 hours
Study and examination requirements:	Homework + presentation or oral examination
Weighting of the grade in the overall grade:	According to the study and examination regulations
Learning outcomes:	After completing this module, students will be able to understand and assess various approaches to the analysis of security situations in an international context, taking into account cultural, political and geographical circumstances and the governance of a security organization in international corporations. They will gain skills for developing security measures when travelling or sending employees abroad. The students will be familiar with the introduction of crisis management, the response in international crisis situations and the management of global crisis communication as well as the public perception of security issues. The students will develop pronounced problem-solving and assessment competence in the areas of:

Contents:	• Security management in global organisations • Travel security • Safety when posting employees • Crisis management in an international environment • Crisis communications: Principles and procedures for communication in crisis situations • Internal and external crisis communication • Message House • Dealing with the media in crisis situations • External effect of safety • Campaigns for security topics
Teaching and learning methods:	Interactive mix of lectures, working and presentation of content, demonstration of concepts, practical tasks in groups, working of own content and role plays.
Literature:	• Leidel, Sven: Handbuch Reisesicherheit, 2014 (ISBN 978-3-735777256) • Ansgar Thießen (publ.): Handbuch Krisenmanagement, 2014 (ISBN 978-3658042929) • Lorenz Steinke: Kommunizieren in der Krise, 2014 (ISBN 978-3658043667) • Stephan Gundel (publ.): Sicherheit für Versammlungsstätten und Veranstaltungen: Ein umfassendes Handbuch zur Sicherheitskonzeption, 2017 (ISBN 978-3415059566) • Wei Ning Zechariah Wong: Business Continuity Management System: A Complete Guide for Implementing ISO 22301, 2014 (ISBN 978-0749469115) • Thomas, Alexander: Interkulturelle Handlungskompetenz, 2011 (978-3-834930156) • Garthwaite, Rosie: Handbuch für die gefährlichsten Orte der Welt, 2011 (978-3-827010360)
Additional information:	//

4. Recht, Compliance und Datenschutz

Modul-Nr./Code:	SM410
Modulbezeichnung:	**Recht, Compliance und Datenschutz**
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	Secman Master, 1. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	//
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Michaela Schröter
Dozent/in:	Dr. Raoul Kirmes M.Sc., CISA, QMA, Beratender Ingenieur für Informationssicherheitstechnik
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 Stunden Vorlesung inklusive Arbeit an Fallbeispielen, 90 h Eigenstudium und 30 h Prüfungsvorbereitung
Lehrform/SWS:	Vorlesung: 60 Stunden (4 SWS)
Studien-/ Prüfungsleistungen:	Klausur und/oder Hausarbeit + Referat oder mündliche Prüfung.
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach dem Modul können die Studierenden die relevanten Rechtslagen für die wesentlichen sicherheitsbezogenen Aktivitäten in Unternehmen verstehen und die Anwendung von nationalen, europäischen und internationalen Rechtsvorschriften zur Erfüllung von Compliance-Vorgaben für Unternehmen verfolgen. Sie erhalten die Befähigung zur kritischen Auseinandersetzung mit rechtlichen Zielkonflikten und zur Abgabe einer angemessenen Beurteilung der Risikosituation für Unternehmen als Regelungsbetroffene. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz auf den Gebieten:

Inhalte:	• Einführung in die juristische Methodik • Europäisches und Intern. Sicherheitsrecht • Einführung in das WTO-Recht (schw. intern. Produktsicherheitsrecht) • System der Grundfreiheiten und nationale Sicherheitsinteressen • Technische Handelshemmnisse im Sicherheitsrecht • Compliance im Intern. Kontext • Intern., europäisches und nat. Akkreditierungsrecht • Grundlagen vertraglicher Haftung (§§280 BGB) • Grundlagen deliktischer Haftung (§§823ff BGB, ProdHaftG) • Recht des privaten Sicherheitsgewerbes • Überblick zum deutschen Waffenrecht • Grundzüge Strafverfahrensrechts • Elektronischer Rechtsverkehr (eCommerce/Signaturrecht) • Intern. Bezüge und Grundlagen des Datenschutzrechtes
Lehr- und Lernmethoden:	Vorlesung
Literatur:	• Harald Jele, Wissenschaftliches Arbeiten: Zitieren, Kohlhammer, 3. Aufl., 2012 • Calliess/Ruffert, EUV/AEUV 6. Auflage 2016. • Europarecht (Mohr Lehrbuch) Taschenbuch – 1. April 2016, Haratsch/Koenig/Pechstein • Röhl, Akkreditierung und Zertifizierung im Produktsicherheitsrecht, Springer Verlag 2000. • Ensthaler, Zertifizierung und Akkreditierung technischer Produkte, Springer Verlag 2007. • Martin Schulte, Handbuch des Technikrechts,2. Aufl. Springer Verlag, 2011. • bbott/ Kirchner/ et.al., International Standards and the Law, Stämpfli Verlag AG, 2005. • Kurt Schellhammer, Schuldrecht nach Anspruchsgrundlagen, Auflage: 9., 2014. • Roggan, Fredrik; Kutscha, Martin: Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, BWV Verlag, 2006. • Rolf Stober, Sven Eisenmenger, Besonderes Wirtschaftsverwaltungsrecht, 16 Aufl., Verlag Kohlhammer, 2016 • Krey/Kapoor, Praxisleitfaden Produktsicherheitsrecht: CE-Kennzeichnung - Risikobeurteilung - Betriebsanleitung - Konformitätserklärung - Produkthaftung - Fallbeispiele Gebundene Ausgabe – 6. November 2014. • Knemeyer: Polizei- und Ordnungsrecht, Beck, 4.Aufl. 2016 • Busche: Waffenrecht 9 Auf. 2016 • Hoeren: Internet- und Kommunikationsrecht, Otto Schmidt Köln 2012 • Schade: Arbeitsrecht, 8 Aufl. Kohlhammer 2016 • Bloehs/Frank Akkreditierungsrecht, C.H.Beck, 2015 • Kugler/Rücker New European General Data Protection Regulation: Ensuring Compliant - Corporate Practice, 2017 • Essentials of WTO Law, Peter Van Den Bossche , 2016 • Spiros Simitis, Bundesdatenschutzgesetz, Nomos, Aufl. 8, 2014 Aktuelle Gesetzestexte
Besonderes:	Intensives Lesepensum

5. Organisatorische Aspekte des Sicherheitsmanagements

Modul-Nr./Code:	SM420
Modulbezeichnung:	**Organisatorische Aspekte des Sicherheitsmanagements**
ggf. Aufteilung in Lehrveranstaltungen:	Unternehmensführung und Sicherheitsstrategie Physische Sicherheit
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	//
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Gerhard Reinhardt, Holger Könnecke
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS:	Vorlesung: 30 h (2 SWS), Übung mit Bearbeitung von Fallbeispielen: 30 h (2 SWS)
Studien-/ Prüfungsleistungen	Praktische Arbeit und Referat und/oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls kennen die Studierenden - im Bereich der Unternehmensführung und Sicherheitsstrategie - die Prinzipien erfolgreicher Unternehmensführung und die Methoden zur Überzeugung der Unternehmensleitung zur Beachtung von Sicherheitsaspekten und zum konstruktiven Umgang mit Krisensituationen. Dafür werden die Fähigkeiten entwickelt, eine Sicherheitsstrategie von den Sicherheitszielen der Unternehmensstrategie abzuleiten, eine Strategie zur Stärkung der ethischen Aspekte der Unternehmensführung zu entwickeln und bei der Lösung von Konflikten zu unterstützen. Nach dem Modulteil zur physischen Sicherheit können die Studierenden verschiedene Ansätze der Schutz- und Sicherheitstechnik, der Analyse der Einsatzmöglichkeiten und Wirkungsweisen von Schutzmechanismen gegen Elementarschäden, mechanischen Sicherheitseinrichtungen, Gefahrenmeldeanlagen und Beobachtungseinrichtungen

	anwenden. Die Lernenden trainieren die Planung eines Sicherheitssystemverbunds mit Bewertung von am Markt angebotenen Lösungen. Weiterhin erhalten sie Kenntnisse zur Einschätzung der rechtlichen Grundlagen für den Einsatz der einzelnen Sicherheitsmechanismen. Die Studierenden trainieren durch die gestellten Aufgaben ihre Teamfähigkeit und ihr Selbstmanagement und entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz auf den Gebieten.
Inhalte:	• Funktionen der Unternehmensführung (Entwicklung von Unternehmensziele, -grundsätze, -kultur; Formulierung von Strategien; Personal- und Verhandlungsführung; internationale Aspekte im globalen Wettbewerb) • Integration von Sicherheitszielen in die Unternehmensstrategie • Ethische Aspekte der Unternehmensführung (Anti-Korruptionsstrategien, Code of Conduct etc.) • Konfliktmanagement (Konfliktdiagnose, Typologie von Konflikten, Eskalationen, Strategien zur Konfliktbehandlung) • Grundlagen der Gebäudesicherheit • Begriffe und Überblick über Aufgabengebiete und Möglichkeiten • Technische Grundlagen • Physische Angriffe und ihre Wirkung • Elementarschäden • Angreifer, Ziele und Angriffsmethoden • Waffen und ihre Wirkung • Abstrahlung elektronischer Geräte • Mechanische Sicherheitseinrichtungen und Zutrittskontrolle • Schlösser, Schließanlagen und ihre Sicherheit • Angriffssicherung an Türen und Fenstern und Zaunanlagen • Wertbehältnisse und Datensicherungsschränke • Technische und rechtliche Vorschriften und Richtlinien • Gefahrenmeldeanlagen • Grundlagen • Einbruchmeldeanlagen • Überfallmeldeanlagen • Technische Störungsmeldeanlagen • Brandmelde- und Brandbekämpfungsanlagen • technische und rechtliche Vorschriften und Richtlinien • Beobachtungseinrichtungen • Technische Möglichkeiten • Offene und verdeckte Überwachung • Technische und rechtliche Vorschriften und Richtlinien • Notfallplanung und betriebliche Sicherheit • Folgeschädenanalyse • Handhabung von Vorfällen
Lehr- und Lernmethoden:	Vorlesung, Bearbeitung von Fallbeispielen in Kleingruppen, Vorstellung von Praxisbeispielen, Rollenspiele.

Literatur:	• Macharzina, K.: Unternehmensführung: Das internationale Managementwissen Konzepte - Methoden – Praxis. 9. Aufl. 2015 • Hutzschenreuther, T.: Krisenmanagement. 2007 • Glasl, F.: Ein Handbuch für Führungskräfte, Beraterinnen und Berater. 11. Aufl. 2017 • Stackpole, B., Osendahl, E.: Security Strategy: From Requirements to Reality, 2010 • Walz, Georg von, Herausgeber: Handbuch der Sicherheitstechnik, Springerverlag, 2012 • Handbuch der Arbeits- und Unternehmenssicherheit in Kreditinstituten, Erich Schmidt-Verlag, 2012 • Kairallah, Michael: Physical Security Systems Handbook, 2005
Besonderes:	//

6. Netzwerksicherheit

Modul-Nr./Code:	SM310
Modulbezeichnung:	**Netzwerksicherheit**
ggf. Aufteilung in Lehrveranstaltungen:	Vorlesung, Übung, Projekt
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	Das Modul kann in anderen Studiengängen entsprechend der dortigen Studien- und Prüfungsordnung verwendet werden.
Häufigkeit des Angebots von Modulen:	jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Eberhard von Faber
Dozent/in:	Prof. Dr. Eberhard von Faber Dipl.-Ing. Dietmar Hausmann
Lehrsprache:	Deutsch
Voraussetzungen:	Bedeutung der IT-Sicherheit und deren Rolle in der Praxis; technische und physikalische Grundkenntnisse; Kenntnisse zu den Grundlagen von Internet-Netzwerken, Betriebssystemen und kryptographiebasierten Techniken
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS:	Vorlesung im Umfang von mindestens 30 Stunden (2 SWS) sowie Übungen von bis zu 30 Stunden (2 SWS)
Studien-/ Prüfungsleistungen:	Prüfung gemäß Rahmenordnung und SPO
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls verfügen die Studierenden über • die Kenntnis über Bedrohungen und Herausforderungen in Netzwerken sowie wichtiger Gegenmaßnahmen in Form von Protokollen und diversen Sicherheitslösungen, • das Verständnis technischer IT-Systeme, deren Interaktion sowie der Identifikation von Schwachstellen und Angriffsvektoren, • die Kenntnis der Funktionsweise von Sicherheitslösungen, Verständnis ihres Einsatzes, Betriebes und Zusammenwirkens; die Fähigkeit, einige dieser Lösungen selbst zu implementieren und einzusetzen; das Verständnis zu Sicherheitsniveaus als System zusammenwirkender technischer und organisatorischer Maßnahmen, • die Fähigkeit, Anforderungen und industrielle Praxisfaktoren zu analysieren und praktische Sicherheitslösungen zu

	beurteilen.
Inhalte:	• Netzwerkprotokolle, Netzwerkdienste und Netzwerkdesign (TCP/IP-Protokollfamilie), Routing und Switching, Identifikation von Sicherheitsproblemen • Kategorien von Bedrohungen, Identifikation von Schwachstellen und Gefährdungen, Grundlagen des Penetration Testing, Tools • Attacken und Gegenmaßnahmen • Sicherheitsmanagement und Standards • Anwendung kryptografischen Verfahren in IT-Systemen (SSL/TLS, IPSec, EAP) Authentifikation, Verschlüsselung, Integritätsschutz • Vertiefung und praktische Anwendung in Projektthemen, Implementierung und Konfiguration technischer Maßnahmen zur Erhöhung der IT-Sicherheit (Routing, Switching, Firewalls, IDS/IPS, Monitoring, Logging, Business Continuity) • Heterogenität moderner Netze, sichere mobile und drahtlose Kommunikation
Lehr- und Lernmethoden:	Vorlesung, Übungen im Labor, Projektarbeit eLearning-Module
Literatur:	Eckert Claudia: IT-Sicherheit Konzepte - Verfahren – Protokolle, Oldenbourg Wissenschaftsverlag GmbH, München, 2014 Kappes Martin: Netzwerk- und Datensicherheit - Eine praktische Einführung, Springer Vieweg, 2013 Studer Bruno: Netzwerkmanagement und Netzwerksicherheit, ein Kompaktkurs für Praxis und Lehre, vdf Hochschulverlag Zürich, 2010 Alexander, Michael: Netzwerke und Netzwerksicherheit - Das Lehrbuch Hüthing Verlag, 10/2006 Paulus Sachar: Basiswissen Sichere Software, dpunkt Verlag, 2011 Badach Aanatol, Hoffmann Erwin: Technik der IP-Netze, Hanser Verlag, 2015 Michael Messner: Hacking mit Metasploit, dpunkt Verlag, 2015 Frank Neugebauer: Penetration Testing mit Metasploit, dpunkt Verlag, 2012 Wendell Odom: CISCO CCENT/CCNA ICND1 100-105, dpunkt.verlag, 2017 CCNA Exploration Companion Guide, Bnd. 1-4 Cisco Network Academy, Addison-Wesley Verlag, 2008. zusätzliche Literatur zu den Projektthemen (VPN, IPSec, IPv6, IPS, WLAN, Angriffe, u.a.m) Bundesamt für Sicherheit in der Informationstechnik, Publikationen, https://www.bsi.bund.de
Besonderes:	Begleitend zur Vorlesung kann das Zertifikat „CCNA-Security" erworben werden

7. Mathematisch-technische Grundlagen der IT-Sicherheit

Modul-Nr./Code:	SM320
Modulbezeichnung:	**Mathematisch-technische Grundlagen der IT-Sicherheit**
ggf. Aufteilung in Lehrveranstaltungen:	Grundlagen von Forensik und Auditing, Grundlagen technischer Sicherheit: Kryptographie
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	Das Modul ist in dem Masterstudiengang Wirtschaftsinformatik als Vertiefungsfach für die Spezialisierungsrichtung „Informationssicherheit" verwendbar.
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Igor Podebrad
Dozent/in:	Prof. Dr. Igor Podebrad, Prof. Dr. Michael Syrjakow
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS:	Vorlesung: 60 Stunden (4 SWS)
Studien-/ Prüfungsleistungen:	Hausarbeit/Klausur/mündliche Prüfung pro Lehrveranstaltung
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden - im Bereich von „Forensik und Auditing" - Kenntnisse und Fertigkeiten zur Anwendung der mathematischen und technischen Grundlagen der Sicherheit, insbesondere der Organisation von IT-forensischen Analysen und IT-Audits und dem Betreiben von IT-Systemen unter Berücksichtigung der Anforderungen an IT-Forensik und IT-Audit. Die Studierenden erhalten die Fähigkeit, IT-Forensik-bezogene Sicherheitsrichtlinien zu entwickeln und durchzusetzen sowie die Kenntnisse zur Bewertung der Verwendbarkeit von IT-Audit-Ergebnissen für Forensik. Im Kontext der „technischen Sicherheit" erhalten die Lernenden Kenntnisse über die symmetrische Verschlüsselung, insbesondere informationstheoretisch sichere Verschlüsselungen, klassische Verschlüsselungsverfahren, Blockchiffren (DES, AES), Stromchiffren, Verschlüsselungsmodi (z. B. CBC), Angriffe. Bei der asymmetrischen Verschlüsselung erhalten sie Kenntnisse zu RSA, Diffie-Hellman-

	Schlüsselaustausch, zahlentheoretischen Grundlagen (Euklidischer Algorithmus, modulare Arithmetik, etc.), Angriffen. Weiterhin erhalten die Studierenden Kenntnisse zur Nachrichtenauthentifizierung, digitalen Signaturen, Public-Key-Infrastruktur (PKI), Angriffen, aktuellen Trends in der Kryptographie (Quantenkryptographie, etc.). Die erworbenen fachlichen und methodischen Kompetenzen zielen auf die Vorbereitung für das Berufsleben ab.
Inhalte:	• Gesetzliche Voraussetzungen für IT-Forensik • Prinzipien von IT-Audit • Organisation von IT-forensischen Analysen • Grundlagen und Anwendungen kryptografischer Verfahren
Lehr- und Lernmethoden:	Vorlesung und Übungen in Kleingruppen.
Literatur:	• Geschonnek, Alexander: IT-Forensik, 2011. • The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons, 2012. • Ertel, Wolfgang: Angewandte Kryptographie; Carl Hanser Verlag, 4. Auflage, 2012. • Paar, Christof, Pelzl, Jan: Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender; Springer Vieweg, 2016. • Schmeh, Klaus: Kryptografie: Verfahren, Protokolle, Infrastrukturen; dpunkt Verlag, 6. Auflage, 2016.
Besonderes:	Im Bereich der Kryptographie: Verwendung des Werkzeugs „CrypTool" zum Experimentieren mit kryptographischen Verfahren.

8. Sichere IKT-Infrastrukturen und IT-Dienste

Modul-Nr./Code:	SM220
Modulbezeichnung:	**Sichere IKT-Infrastrukturen und IT-Dienste**
ggf. Aufteilung in Lehrveranstaltungen:	Teil A (WiSe), „Grundlagen und Anwendungen der Kryptographie und des Identitäts- und Zugriffsmanagements (IAM)" Teil B (SoSe), „Sicherheitslösungen, IT Outsourcing, Cloud, industrielle IT-Produktion und sichere IT-Dienste"
Dauer des Moduls:	Zweisemestrig
Zuordnung zum Curriculum:	SecMan Master, 1. und 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	Die beiden Lehrveranstaltungen des Moduls sind soweit in sich abgeschlossen, dass sie in beliebiger Reihenfolge belegt werden können.
Häufigkeit des Angebots von Modulen:	jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Eberhard von Faber
Dozent/in:	Prof. Dr. Eberhard von Faber
Lehrsprache:	Deutsch
Voraussetzungen:	Bedeutung der IT-Sicherheit und deren Rolle in der Praxis, technische und physikalische Grundkenntnisse, Kenntnisse zur Informations- und Kommunikationstechnologie: Anwendungen, Systeme und Netze sowie zugrundeliegende Technologien.
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS:	Vorlesung mit gemischten Medien, Angebot von Selbststudium und Hausaufgabe zur Vertiefung und Selbstkontrolle sowie Kontrollfragen/Repetitorium. 2 x 2 SWS in vier Blöcken
Studien-/ Prüfungsleistungen:	Klausur oder mündliche Prüfung jeweils über Teil A und B (zwei Prüfungen)
Gewichtung der Note in der Gesamtnote:	Laut SPO

Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden grundlegende Kenntnisse und Fähigkeiten auf den folgenden Gebieten. **Teil A - Grundlagen und Anwendungen der Kryptographie und des Identitäts- und Zugriffsmanagements (IAM):** Die Studierenden entwickeln die Fähigkeit, Anforderungen und industrielle Praxisfaktoren zu analysieren und Lösungen auch in Branchenlösungen zu integrieren. Zudem erlernen sie Grundlagen der Kryptografie und ihre praktische Anwendung sowie die Grenzen bzw. die Aufgaben für das Schlüsselmanagement. Die Lernenden gewinnen detaillierte Kenntnisse auf dem Gebiet „Identity and Access Management (IAM)". Weiterhin verfügen sie über die Grundbegriffe sowie Architekturen und Technologien für Unternehmen und in komplexen Wertschöpfungsketten. **Teil B - Sicherheitslösungen, IT Outsourcing, Cloud, industrielle IT-Produktion und sichere IT-Dienste:** Die Studierenden erlangen grundsätzliche Kenntnisse und Fertigkeiten, um zu verstehen, wie Anforderungen systematisch analysiert und umgesetzt werden, sowie die Fähigkeit, selbst Sicherheit zu konzipieren und zu bewerten. Die Lernenden erlangen Kenntnisse und Fertigkeiten zur Absicherung einer (industriellen) IT-Produktion sowie zur Beschaffung und Nutzung von IT-Diensten durch die Anwenderorganisationen (Bewertung, Auswahl, Aufrechterhaltung, GRC). Sie entwickeln ein Verständnis der wichtigsten Sicherheitsaufgaben entlang des Lebenszyklus der Geschäftsbeziehung und deren Ausgestaltung durch Anwender und Dienstleister. Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz.
Inhalte:	**Teil A - Grundlagen und Anwendungen der Kryptographie und des Identitäts- und Zugriffsmanagements (IAM):** • Lernbeispiel der speziellen Branchen-Anwendung „Bezahlsysteme": Anforderungen und Lösungen; Praxisfaktoren und Auswirkungen, industrielle Praxis • Grundlagen der Kryptografie; Schlüsselmanagement • Absicherung von Geschäftsprozessen; Grundbegriffe IAM (alles von Administration bis Accounting), • Autorisierung: Leistungen und Grenzen; Strategien (DAC, MAC, RBAC, IF); Realisierung (Gruppen, Rollen, ACL, Capabilities); Alternativen; Trends und Ausblick, • Authentisierung: Arten, Methoden, Technologien; Probleme und Lösungen; Architekturen und verteilte Systeme (z. B. LDAP, RADIUS, Kerberos, ESSO, Single Sign-On, Federation), • IAM-Architekturen (das ganze Bild) **Teil B - Sicherheitslösungen, IT-Outsourcing, Cloud, industrielle IT-Produktion und sichere IT-Dienste:** • Grundbegriffe der Informationssicherheit; Design-Ziele und Methoden zur Entwicklung adäquater Sicherheitsmaßnahmen • Lieferketten in der IT, Bereitstellungsmodelle und Trends;

	Übersicht über IT-Sicherheitslösungen; Integration der verschiedenen Lösungen im ITK-Verbund • Implikationen der Übertragung von IT-Services an Dritte (IT-Dienstleister); Notwendigkeit und Grundkonzepte des Joint Security Managements (JSM) • Sicherheitsmaßnahmen ordnen und Arbeitsteilung unterstützen: ESARIS Security Taxonomy; technische und prozessuale Sicherheitsmaßnahmen • Beschaffung, Verträge und andere grundlegende Aufgaben • Zusammenarbeit zwischen Anwenderorganisation und IT-Dienstleister in jedem der neun Aufgabenbereiche des JSM; Details in Form einer Gebrauchsanweisung
Lehr- und Lernmethoden:	Kombination aus Vorlesung, Aufgaben und Übungsbeispielen, Vorlesung mit gemischten Medien, Kontrollfragen/ Repetitorium sowie Hausaufgaben.
Literatur:	Teil A: • Anderson, Ross: Security Engineering, "A Guide to Building Dependable Distributed Systems", John Wiley & Sons • Alexander Tsolkas und Klaus Schmidt: „Rollen und Berechtigungskonzepte, Ansätze für das Identity- und Access Management im Unternehmen", 2010, Vieweg+Teubner • Claudia Eckert: „IT-Sicherheit, Konzepte - Verfahren – Protokolle", Oldenbourg-Verlag, 2013 Teil B: • Eberhard von Faber and Wolfgang Behnsen: "Secure ICT Service Provisioning for Cloud, Mobile and Beyond", Springer-Vieweg. zweite, völlig neue Auflage 2017 • Eberhard von Faber, Wolfgang Behnsen: Joint Security Management: organisationsüber-greifend handeln; ISBN 978-3-658-20833-2, 244 Seiten, 60 farbige Abbildungen, neu 2018 • Datenschutz und Datensicherheit, DuD, Heft 10/2016: Schwerpunkt „Informationssicherheit beim IT-Outsourcing", Herausgegeben von Eberhard von Faber, diverse Beiträge auf ca. 40 Seiten, Springer, ISSN 1614-0702 • Open Enterprise Security Architecture (O-ESA), The Open Group, Van Haren Publ., 2011, ISBN 978 90 8753 672 5 • Martin Kappes: „Netzwerk- und Datensicherheit, Eine praktische Einführung", Vieweg+Teubner • Common Criteria for Information Technology Security Evaluation; www.commoncriteriaportal.org oder ISO 15408 • www.itil.org Skripte und andere Lehrmaterialien werden während der Vorlesung direkt an die Studierenden verteilt.
Besonderes:	//

9. Secure Systems Lifecycle Management

Modul-Nr./Code:	SM230
Modulbezeichnung:	**Secure Systems Lifecycle Management (SSLM)**
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	Das Modul kann auch als WPF für Wirtschaftsinformatik und Informatik Master angeboten werden.
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller, Sandro Hartenstein
Lehrsprache:	Deutsch und Englisch
Voraussetzungen:	Erste Erfahrungen im Programmieren von Web-Anwendungen für das Beispiel-Szenario. Dies sollte i.d.R. durch das bis zu diesem Zeitpunkt absolvierte Studium sichergestellt sein. Ansonsten: Selbststudium, z. B. mit PHP 7 und MySQL: Von den Grundlagen bis zur professionellen Programmierung von Christian Wenz und Tobias Hauser (April 2016); Einstieg in JavaScript: Dynamische Webseiten erstellen inkl. Zusammenspiel von HTML, CSS, Ajax, jQuery, jQuery mobile u.v.m. von Thomas Theis (Februar 2016)
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS:	30 h Vorlesung (2 SWS), 30 h Übungen (2 SWS)
Studien-/ Prüfungsleistungen:	Praktische Arbeit und Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	Laut SPO

Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden Kenntnisse und Fertigkeiten zu: • Best Practices sowie bestehenden Frameworks während der Entwicklung von IT-basierten Systemen für sichere Software • Entwicklung von Akzeptanzkriterien für nicht-funktionale Sicherheitsanforderungen • Durchführung von Bedrohungsmodellierungen • Vermeidung von Schwachstellen während der Entwicklung • Durchführung von Sicherheitstests • Sicherem Installieren und Betreiben von Software • Etablierung eines Security Response Programms • Analyse von bestehender Software auf Sicherheitsschwachstellen • Entwicklung und Umsetzung eines Schutzprogramms für Software während der Systementwicklung • Etablierung eines Management-Systems für Sicherheit im Entwicklungsprozess, Integrieren dieses Management-Systems in einen ggf. vorhandenen Qualitätsprozess • Durchführung von Sicherheitsanalysen („Hacking") • Darstellung von Untersuchungsergebnissen Sie beherrschen die theoretischen Grundlagen, um diese kognitiv, intuitiv und kreativ in der Studienarbeit umzusetzen und trainieren durch die gestellten Aufgaben ihre Teamfähigkeit und ihr Selbstmanagement.
Inhalte:	Grundsätze der sicheren Software-Entwicklung: • Sicherheitsanforderungen • Sicheres Design und Bedrohungsmodellierung • Architekturanalysen • Sicheres Kodieren • Sicherheitstests • Sichere Einrichtung • Security Response • Schutz der eigenen Software vor Manipulation und Know-how-Diebstahl
Lehr- und Lernmethoden:	Interaktiver Mix aus Vorlesung, Übungen am eigenen Computer, Übungen im Labor, Erarbeiten und Vortragen von Inhalten, Demonstration von Konzepten, praktischen Aufgaben in Gruppen.
Literatur:	• Paulus, Sachar M. (2011), „Basiswissen Sichere Software. Aus- und Weiterbildung zum ISSECO Certified Professional for Secure Software Engineering", 1., neue Ausg. Heidelberg, Neckar: Dpunkt (ISQL-Reihe). • Müller, Klaus-Rainer (2014): „IT-Sicherheit mit System, Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sicherheitspyramide – Standards und Practices – SOA und Softwareentwicklung". 5., neu bearb. U. erg. Aufl. Wiesbaden: Springer Vieweg. • Shoestack, A.: threat modeling, designing for security, John Wiley & Sons, 2014. • Metasploit: "A Penetration Tester's Guide", Kennedy, No Starch Press, 2011. • F. Long, JAVA Coding Guidelines, Addison-Wesley, 2013. • M. Howard, D. DeBlanc, Sichere Software programmieren, Microsoft Press, 2002.

	• J. Caballero, Engineering Secure Software and Systems, 8th intl. Symposium ESSoS16, Springer, 2016. • Lipner, S.: The trustworthy computing security development lifecycle, in: Computer Security Applications Conference, 2004. 20th Annual Conference, S. 2-13, 2004.
Besonderes:	Weitere Vertiefung ist in den Pflichtgebieten „Wissenschaftliches Arbeiten" und „Projekt" möglich

Module no./code:	SM230
Module description:	**Secure systems lifecycle management (SSLM)**
Division into teaching sessions, if applicable:	//
Duration of module:	One semester
Classification in the curriculum:	SecMan master, 2nd semester, core module
Usability of the module:	The module can also be offered as WPF for the business studies and informatics masters.
Frequency offered:	Every academic year
Module leader:	Prof. Dr. Ivo Keller
Lecturer:	Prof. Dr. Ivo Keller, Sandro Hartenstein
Language of instruction:	German and English
Prerequisites:	Initial experience in programming web applications for the example scenario. This should generally be assured through completion of the degree up to that date. Otherwise: Self-study, e.g. with PHP 7 and MySQL: Von den Grundlagen bis zur professionellen Programmierung by Christian Wenz and Tobias Hauser (April 2016); Einstieg in JavaScript: Dynamische Webseiten erstellen inkl. Zusammenspiel von HTML, CSS, Ajax, jQuery, jQuery mobile u.v.m. by Thomas Theis (February 2016)
ECTS credits:	6
Total workload and composition of course:	180 hrs. = 60 hrs. attendance, 120 hrs. self-study (incl. examination preparation and examination)
Form of teaching/semester hours per week:	30 hrs. lectures, 30 hrs. workshops
Study and examination requirements:	Practical work and presentation or oral examination
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 the knowledge and skills of: • Best practices and existing frameworks during the development of IT-based systems for secure software • Development of acceptance criteria for non-functional safety requirements • Conducting threat modelling • Avoiding weak spots during development • Conducting security tests • Safe installation and operation of software • Establishment of a security response program • Analysis of existing software for security vulnerabilities • Development and implementation of a software protection program during system development • Establishment of a management system for safety in the development process, integration of this management system into any existing quality process • Conducting security analyses ("hacking") • Presentation of examination results They will master the theoretical foundations in order to implement them cognitively, intuitively and creatively in the degree thesis and train their teamwork and self-management through the tasks they set themselves.
Contents:	Principles of secure software development: • Security requirements • Secure design and threat modelling • Architecture analysis • Secure coding • Security testing • Secure facilities • Security response • Protection of own software against manipulation and theft of specialist knowledge
Teaching and learning methods:	Interactive mix of lectures, workshops using your own computer, workshops in the lab, preparation and presentation of content, demonstration of concepts, practical group tasks.
Literature:	• Paulus, Sachar M. (2011), "Basiswissen Sichere Software. Aus- und Weiterbildung zum ISSECO Certified Professional for Secure Software Engineering", 1st, new ed. Heidelberg, Neckar: Dpunkt (ISQL series). • Müller, Klaus-Rainer (2014): "IT-Sicherheit mit System, Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sicherheitspyramide – Standards und Practices – SOA und Softwareentwicklung". 5th, revision and updated edition, Wiesbaden: Springer Vieweg. • Shoestack, A: threat modeling, designing for security, John Wiley & Sons, 2014 • Metasploit: "A Penetration Tester's Guide", Kennedy, No Starch Press, 2011 • F. Long, JAVA Coding Guidelines, Addison-Wesley, 2013 • M. Howard, D. DeBlanc, Sichere Software programmieren, Microsoft Press, 2002 • J. Caballero, Engineering Secure Software and Systems, 8th

	intl. Symposium ESSoS16, Springer, 2016 • Lipner, S.: The trustworthy computing security development lifecycle, in: Computer Security Applications Conference, 2004. 20th Annual Conference, S. 2-13, 2004.
Additional information:	Additional deepening of knowledge is possible in the core areas of "Scientific work" and "Project"

10. Wissenschaftliches Schreiben

Modul-Nr./Code:	SM510
Modulbezeichnung:	**Wissenschaftliches Schreiben**
ggf. Aufteilung in Lehrveranstaltungen:	Semesterarbeit, Management-Report
Dauer des Moduls:	Zweisemestrig
Zuordnung zum Curriculum:	SecMan Master, 1. und 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	//
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenzstudium, Konsultationen und 120 h betreutes Erstellen einer Ausarbeitung
Lehrform/SWS:	Vorlesung und Seminar mit Referat: 60 Stunden; 2 x 2 SWS
Studien-/ Prüfungsleistungen:	Schriftliche Arbeit
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls sind die Studierenden in der Lage, wissenschaftliche Arbeiten im Themenfeld der Sicherheit zu erstellen. Für den Management-Report wird der Inhalt einer normalen wissenschaftlichen Ausarbeitung auf max. 7.500 Anschläge verdichtet. Die erworbenen fachlichen und methodischen Kompetenzen zielen auf die Vorbereitung für das Berufsleben ab.
Inhalte:	• Erhebungsmethoden (Statistik, Interview, primär/sekundär Quellen) • Quellendiskussion: recherchieren, lesen, bewerten • Kreativitätstechniken und Selbstorganisation • situationsbezogene Anforderungen an Schreibstile (Werbung, Pressemitteilung, wiss. Arbeit …) • Erstellung eines Exposés • Methodischer Aufbau wiss. Arbeiten • Struktur, roter Faden und Folgerichtigkeit • Materialsammlung und Recherche • Materialbewertung und –auswahl • Zitiersysteme

	• Branchenspezifische orthographische Probleme • Managementgerechtes Präsentieren
Lehr- und Lernmethoden:	Vorlesung, Stil- und Strukturierungsübungen, Diskussion, Vorstellen der eigenen Ergebnisse.
Literatur:	• DIN 1421 (Gliederung und Benummerung in Texten) • Karmasin, M.; Ribing, R.: Die Gestaltung wissenschaftlicher Arbeiten: Ein Leitfaden für Seminar-arbeiten, Bachelor-, Master- und Magisterarbeiten sowie Dissertationen. 6. Auflage Stuttgart: UTB, 2017 • Rehborn, A.: Fit für die Prüfung: Wissenschaftliches Arbeiten. Konstanz: UVK, 2013 • Esselborn-Krumbiegel, Helga: „Richtig wissenschaftlich schreiben", Uni Tipps, Band 3429, 5. Auflage, Verlag Ferdinand Schöningh, April 2017 • Kornmeier, Martin: „Wissenschaftlich schreiben leicht gemacht-für Bachelor, Master und Dissertation", 7. Aufl. Bern, Haupt Verlag, 2016 • Bortz, Jürgen, Döring, Nicola: „Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler", 3. Aufl. Berlin, Springer Verlag, 2003 • Eco, Umberto: „Wie man eine wissenschaftliche Abschlußarbeit schreibt", facultas wuv UTB, 13. Auflage 2010 • Mautner, Gerlinde: „Wissenschaftliches Englisch", 2. Aufl., 2016, Verlag Huter & Roth KG, utb
Besonderes:	//

11. Projekt

Modul-Nr./Code:	SM530
Modulbezeichnung:	**Projekt**
ggf. Aufteilung in Lehrveranstaltungen:	//
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	//
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller
Lehrsprache:	Deutsch
Voraussetzungen:	//
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 90 h Eigenstudium und 30 h Referatsvorbereitung („Verteidigung“)
Lehrform/SWS:	Vorlesung, Seminar und Betreuung der Projektgruppen: 60 Stunden
Studien-/ Prüfungsleistungen:	Praktische Arbeit mit Referat
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden die Fähigkeiten zur • Planung eines sicherheitsbezogenen Projekts unter ganzheitlicher Beachtung der Anforderungen • Durchführung von Sicherheitsprojekten • Anwendung von Projektmanagement-Methoden Die Studierenden trainieren durch die gestellten Aufgaben ihre Teamfähigkeit und ihr Selbstmanagement. Die erworbenen fachlichen und methodischen Kompetenzen zielen auf die Vorbereitung für das Berufsleben ab.

Inhalte:	• Problemerkennung: - wissenschaftliche Erarbeitung des „State of the Art" - Einbindung in den vorhandenen praktischen Kontext - Rahmenbedingungen des Einsatzes • Nutzung unterschiedlicher Analysetechniken wie bspw. Interviewmethode, Fragebogen Delphi-Methode, Erarbeitung des Kontextes über Dokumente usw. • Sollkonzeptentwicklung: - wissenschaftlich fundierte Entwicklung eines praxisorientierten Lösungsansatzes - Nutzung von Kreativitätsmethoden - Kosten-/Nutzen-Analysen - Entwicklung von Rahmenbedingungen des Einsatzes • Prototypische Umsetzung - die prototypische Umsetzung erfolgt durch Entwicklung eines Software-Prototypen - Umsetzung im Unternehmen bzw. Organisation oder Entwicklung bspw. eines Antrags auf Forschungs- und Entwicklungsförderung
Lehr- und Lernmethoden:	Vorlesung, praktisches Arbeiten in Gruppen mit maximal 5 Teilnehmern, Vorstellen der eigenen Ergebnisse
Literatur:	• "A Guide of the Project Management Body of Knowledge", Project Management Institute, 5th edition, 2013 • Krallmann, Herrmann: „Systemanalyse im Unternehmen – Prozessorientierte Methoden der Wirtschaftsinformatik", 6. Auflage, 2013, Oldenburg Wissenschaftsverlag • App, S.: „Virtuelle Teams", Haufe TaschenGuide, 2013 • Nowotny, Valentin: „AGILE UNTERNEHMEN – FOKUSSIERT, SCHNELL, FLEXIBEL: Nur was sich bewegt, kann sich verbessern", 2. Auflage, 2017, BusinessVillage • Bobikiewicz, Lucius: „Virtual Meeting [Vting]: Ein Praxisbuch für verteilte Teams", Loop-2, 2014 • Spezial-Literatur zum Projektthema wird im Rahmen der Lehrveranstaltung benannt.
Besonderes:	Die Bereitschaft zu praktischem Arbeiten bei Kooperationspartnern und zur Zusammenarbeit mit den Projektmitgliedern wird vorausgesetzt.

12. Masterarbeit

Modul-Nr./Code:	SM6100/6300
Modulbezeichnung:	**Masterarbeit incl. Kolloquium**
ggf. Aufteilung in Lehrveranstaltungen:	Masterarbeit Master-Kolloquium
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 3. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	Das Modul dient dem Abschluss des Studiums
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Modulverantwortliche/r:	Prof. Dr. Ivo Keller
Dozent/in:	Der Erstgutachter einer Master-Arbeit muss ein Professor der Technischen Hochschule Brandenburg sein. Der Zweitgutachter wird in Abstimmung mit dem Erstgutachter ausgewählt
Lehrsprache:	Deutsch oder Englisch (nach Wahl der Studierenden/des Studierenden)
Voraussetzungen:	Zur Master-Arbeit kann sich grundsätzlich nur anmelden, wer alle Prüfungsleistungen bis auf die Wahlpflichtmodule erfolgreich absolviert hat.
ECTS-Credits:	21
Gesamtworkload und ihre Zusammensetzung:	600 h Erarbeitung der Thesis inkl. Konsultationen
Lehrform/SWS:	Betreute Erarbeitung der Thesis
Studien-/Prüfungsleistungen:	Masterarbeit (87,5 %) Kolloquium (12,5 %)
Gewichtung der Note in der Gesamtnote:	Laut SPO
Lernergebnisse:	Die Studierenden sind in der Lage, unter Anleitung, in einem Zeitraum von 4 Monaten (in Teilzeit von 8 Monaten), eine wissenschaftliche Arbeit mit eigenen kreativen und/oder konstruktiven Anteilen im Themenfeld des „Security Management" zu erstellen. Das Master-Kolloquium dient der Präsentation der Masterarbeit; im Rahmen dieser mündlichen Prüfung stellt der Kandidat die Ergebnisse seiner Masterarbeit vor und verteidigt diese vor dem Plenum.

Inhalte:	Die Masterarbeit dient der zusammenhängenden Beschäftigung mit einem umfassenden Thema und der daraus resultierenden Lösung einer theoretischen oder praktischen Problemstellung. Im Rahmen des Kolloquiums findet eine mündliche Prüfung und Diskussion statt.
Lehr- und Lernmethoden:	Selbststudium unter Anleitung. Masterarbeit: Eigene wissenschaftliche Arbeit Kolloquium: Vorbereiten eines Vortrags und einer Diskussion, Erstellen von Präsentationsmedien
Literatur:	• Booth, W. C. et al. (1995). The draft of research. Chicago London • Brown, S. R. et al. (1990) Experimental Design and Analysis. London • Cialdini, R. B. (2001). Influence, Science and Practice. Bosten, M.A. • Hussley, J., Hussley, R. (1997). Business Research. A practical guide for undergraduate and postgraduate students • Karmasin, M. et al. (1999). Die Gestaltung wissenschaftlicher Arbeiten. Wien • Pyrczak, S. et. al. (1998). Writing empirical Research Reports. Los Angeles. C.A. • Seale, Clive : "Qualitative Research Practice", 2006, Sage Publications Ltd., London
Besonderes:	//

Module no./code:	SM6100/6300
Module description:	**Master's thesis incl. Master's seminar**
Division into teaching sessions, if applicable:	Master's thesis Master's colloquium
Duration of module:	One semester
Classification in the curriculum:	SecMan master, 3nd semester, core module
Usability of the module:	The module is intended to complete the degree programme
Frequency offered:	Every academic year
Module leader:	Prof. Dr. Ivo Keller
Lecturer:	The first examiner of a Master's thesis must be a professor at Technische Hochschule Brandenburg. The second examiner will be selected in coordination with the first examiner
Language of instruction:	German or English (choice of the student)
Prerequisites:	As a matter of principle, you can only register for the master's thesis if you have successfully completed all examinations except for the elective modules.
ECTS credits:	21
Total workload and composition of course:	600 hrs. writing of the thesis including consultations
Form of teaching/semester hours per week:	Supervised development of the thesis
Study and examination requirements:	Master's thesis (87.5 %) Colloquium (12.5 %)
Weighting of the grade in the overall grade:	According to the study and examination regulations
Learning outcomes:	The students will be able to create a scientific paper with their own creative and/or constructive contributions in the field of "Security management" within a period of 4 months (part time of 8 months). The master's colloquium serves to present the master's thesis; In the course of this oral examination, the candidate presents the results of his master's thesis and defends it in a plenary.
Contents:	The master's thesis serves the associated occupation by way of a comprehensive topic with the resulting solution of a theoretical or practical problem. During the colloquium there will be an oral examination and discussion.
Teaching and learning methods:	Self-study under supervision

	Master's thesis: Own scientific thesis Colloquium: Preparation of a presentation and a discussion, creation of presentation media
Literature:	• Booth, W. C. et al. (1995). The draft of research. Chicago London • Brown, S. R. et al. (1990). Experimental Design and Analysis. London • Cialdini, R. B. (2001). Influence, Science and Practice. Bosten, M.A. • Hussley, J., Hussley, R. (1997). Business Research. A practical guide for undergraduate and postgraduate students • Karmasin, M. et al. (1999). Die Gestaltung wissenschaftlicher Arbeiten. Vienna • Pyrczak, S. et. al. (1998). Writing empirical Research Reports. Los Angeles. C.A. • Seale, Clive : "Qualitative Research Practice", 2006, Sage Publications Ltd., London
Additional information:	//