Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Modulkatalog Pflichtfächer M. Sc. Security Management (SPO 2014/2015)

März 2016

Impressum

Autor:	Max Luber
Redaktion:	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 - 290 F +49 3381 355 - 199 E ivo.keller@th-brandenburg.de www.th-brandenburg.de
Stand:	21. März 2016

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument enthält die Beschreibungen der Pflichtfächer des Masterstudiengangs *Security Management* der Technischen Hochschule Brandenburg in der Version der Studien- und Prüfungsordnung von 2014 und 2015. Die Beschreibungen der Wahlpflichtfächer sind in separate Dokumente ausgegliedert, da diese sich regelmäßig ändern.

Modulübersicht (Regelstudienplan Vollzeit)

<table>
<tr><th>Sem.</th><th colspan="6">Module</th><th>∑ CP</th></tr>
<tr><td>1</td><td>Grundlagen des Security Management (6CP)</td><td>Recht, Compliance und Datenschutz (6CP)</td><td rowspan="2">Sichere IKT-Infra-strukturen und IT-Dienste (6CP)</td><td>Mathematisch-technische Grundlagen der IT-Sicherheit (6CP)</td><td>Netzwerksicherheit (6CP)</td><td rowspan="2">Wissen-schaft-liches Schrei-ben (6CP)</td><td>30</td></tr>
<tr><td>2</td><td>Security- und Krisenmanagement im internationalen Kontext (6CP)</td><td>Organisatorische Aspekte des Sicherheits-management (6 CP)</td><td>Secure Software Lifecycle Management (6CP)</td><td>Projekt (6CP)</td><td>30</td></tr>
<tr><td rowspan="2">3</td><td colspan="2">Wahlpflichtmodul 1 (3CP)</td><td colspan="2">Wahlpflichtmodul 2 (3CP)</td><td>Wahlpflichtmodul 3 (3CP)</td><td>9</td></tr>
<tr><td colspan="5">Masterarbeit incl. Kolloquium (21CP)</td><td>21</td></tr>
<tr><td></td><td colspan="6"></td><td>90</td></tr>
</table>

Fach

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

Modulübersicht (Regelstudienplan Teilzeit)

<table>
<tr><th>Sem.</th><th>Module</th><th></th><th></th><th></th></tr>
<tr><td>1</td><td>Grundlagen des Security Management
(6CP)</td><td>Mathematisch-technische Grundlagen der
IT-Sicherheit
(6CP)</td><td rowspan="2">Sichere IKT –
Infrastrukturen und
IT-Dienste
(6CP)</td><td>15</td></tr>
<tr><td>2</td><td>Security- und Krisenmanagement im internationalen Kontext
(6CP)</td><td>Organisatorische Aspekte des Sicherheits-management (6 CP)</td><td>15</td></tr>
<tr><td>3</td><td>Netzwerksicherheit
(6CP)</td><td>Recht, Compliance und Datenschutz
(6CP))</td><td rowspan="2">Wissenschaftliches Schreiben
(6CP)</td><td>15</td></tr>
<tr><td>4</td><td>Secure Software Lifecycle Management
(6CP)</td><td>Projekt
(6CP</td><td>15</td></tr>
<tr><td rowspan="2">5</td><td>Wahlpflichtmodul 1 (3CP)</td><td colspan="2">Wahlpflichtmodul 2 (3CP)</td><td>6</td></tr>
<tr><td colspan="3">Masterarbeit incl. Kolloquium (21CP)</td><td></td></tr>
<tr><td>6</td><td>Wahlpflichtmodul 3 (3CP)</td><td colspan="2"></td><td>24</td></tr>
<tr><td></td><td></td><td></td><td></td><td>90</td></tr>
</table>

Fach

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

2. Grundlagen des Security Management

Modul-Kurzkennzeichen	SM_MA_GrundlagenSecurityManagement
Modulbezeichnung	Grundlagen des Security Management
ggf. Aufteilung in Lehrveranstaltungen	
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SM Ma, 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
Autor/in	Prof. Dr. Friedrich Holl
Dozent/in	Prof. Dr. Friedrich Holl, Prof. Dr. Heinz-Dieter Schmelling
Lehrsprache	Deutsch
Voraussetzungen	Keine
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz- und 120 h Eigenstudium
Lehrform/SWS	Vorlesung: 15 Stunden, Übung: 15 Stunden, Praktische Anwendung an Fallbeispielen: 30 Stunden
Studien-/ Prüfungsleistungen	Hausarbeit + Referat, alternativ mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote

Lernergebnisse	Die Lernenden sollen in die Lage versetzt werden, die folgenden grundsätzlichen Kenntnisse und Fertigkeiten zu erlangen: • Erstellen von Sicherheitsuntersuchungen • Durchführen von Risikobewertungen • Analysieren von Sicherheitslagen und der Sinnhaftigkeit von Gegenmaßnahmen • Verständnis entwickeln für die Bedeutung der Sicherheit im Entscheidungsprozess bei Unternehmern • Sicherheitsorganisationen im Unternehmen beurteilen • Beispielhaft Sicherheitsprozesse unter Zuhilfenahme von IT-Werkzeugen abbilden • Sicherheitsmaßnahmen erarbeiten und vor einem Entscheidungsgremium erfolgreich durchsetzen Zusätzlich sollen die folgenden Lernergebnisse erreicht werden: • Etablieren einer Sicherheitsorganisation in einem Unternehmen • Erstellen eines Qualifikationsprofils für einen Sicherheitsverantwortlichen • Integrieren von IT- und nicht-IT-Sicherheits-relevanten Aspekten • Einführen eines Sicherheitsmanagementsystems in einer Organisation • Erarbeiten einer Strategie für einen Teilbereich der IT-, Informations- oder Unternehmenssicherheit
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	• Security Management 2011: Handbuch für Informationsschutz, IT-Sicherheit, Standortsicherheit, Wirtschaftskriminalität und Managerhaftung von Guido Birkner, 2011. • Handbuch Unternehmenssicherheit: Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System von Klaus-Rainer Müller, 2010. • Unternehmenssicherheit von Stephan Gundel, und Lars Mülli, 2009. • Security Risk Management Body of Knowledge von Julian Talbot, Miles Jakeman, Wiley 2009.

Besonderes	

3. Security- und Krisenmanagement im internationalen Kontext

Modul-Kurzkennzeichen	SM_MA_SecurityKrisenManagementInternational
Modulbezeichnung	Security- und Krisenmanagement im internationalen Kontext
ggf. Aufteilung in Lehrveranstaltungen	
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SM Ma, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls	
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Friedrich Holl
Dozent/in	Prof. Dr. Friedrich Holl, Prof. Dr. Heinz-Dieter Schmelling
Lehrsprache	Deutsch, z. T. Englisch (10%)
Voraussetzungen	Keine
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz- und 120 h Eigenstudium
Lehrform/SWS	Vorlesung: 60 Stunden, Übung: 30 Stunden, Praktische Anwendung an Fallbeispielen: 30 Stunden
Studien-/ Prüfungsleistungen	Hausarbeit + Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	Die Lernenden sollen in die Lage versetzt werden, die folgenden grundsätzlichen Kenntnisse und Fertigkeiten zu erlangen: Analysieren von Sicherheitslagen im internationalen Kontext unter Berücksichtigung kultureller, politischer und geographischer Gegebenheiten Führen einer Sicherheitsorganisation in internationalen Konzernen Erarbeiten von Sicherheitsmaßnahmen bei Reisen oder Entsendung von Mitarbeitern ins Ausland Einführen eines Krisenmanagements Reagieren in internationalen Krisensituationen Steuern der globalen Krisenkommunikation Beeinflussen der öffentlichen Wahrnehmung zu Sicherheitsthemen

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	Notfall- und Krisenmanagement im Unternehmen von Axel Bédé, 2009. Unternehmenskrisen und Krisenmanagement von Ronny Scharschmidt, 2009. Führen in Krisensituationen von Markus Klaus, 2008. Global Threat: Target-Centered Assessment and Management von Robert Mandel, 2008. Security Risk Management Body of Knowledge von Julian Talbot und Miles Jakeman, 2009.
Besonderes	

4. Recht, Compliance und Datenschutz

Modul-Kurzkennzeichen	SM_MA_RechtComplianceDatenschutz
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
Autor/in	Prof. Dr. Friedrich Holl
Dozent/in	Prof. Dr. Michaela Schröter, Dr. Raoul Kirmes M.Sc., CISA, QMA
Lehrsprache	Deutsch
Voraussetzungen	
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz- und 120 h Eigenstudium
Lehrform/SWS	Vorlesung: 60 Stunden
Studien-/ Prüfungsleistungen	Klausur und/oder Hausarbeit + Referat oder mündliche Prüfung.
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Erlangung von Fertigkeiten zum Erkennen der relevanten Rechtslage für die wesentlichen sicherheitsbezogenen Aktivitäten in Unternehmen • Anwenden von nationalen , europäischen und internationalen Rechtsvorschriften zur Erfüllung von Compliance-Vorgaben für Unternehmen • Befähigung zur kritischen Auseinandersetzung mit rechtlichen Zielkonflikten und zur Abgabe einer angemessenen Beurteilung der Risikosituation für Unternehmen als Regelungsbetroffene

Inhalte	• Einführung in die juristische Methodik • Europäisches und Int. Sicherheitsrecht • Einführung in das WTO-Recht (schw. int. Produktsicherheitsrecht) • System der Grundfreiheiten und nationale Sicherheitsinteressen • Technische Handelshemmnisse im Sicherheitsrecht • Compliance im Int. 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) • Int. Bezüge und Grundlagen des Datenschutzrechtes
Lehr- und Lernmethoden	Vorlesung

Literatur	• Harald Jele, Wissenschaftliches Arbeiten: Zitieren, Kohlhammer, 3. Aufl., 2012 • Calliess/Ruffert, EUV/AEUV 4. Auflage 2011. • 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, 2010. • bbott/ Kirchner/ et.al., International Standards and the Law, Stämpfli Verlag AG, 2005. • Kurt Schellhammer, Schuldrecht nach Anspruchsgrundlagen, Auflage: 8.,2011. • Martin Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, BWV Verlag, 2006. • olf Stober, Sven Eisenmenger, Besonderes Wirtschaftsverwaltungsrecht, 15 Aufl., Verlag Kohlhammer, 2011 • Knemeyer: Polizei- und Ordnungsrecht, Beck, 2007 • Busche: Waffenrecht 2012, Kiel 2012 • Hoeren: Internet- und Kommunikationsrecht, Otto Schmidt Köln 2012 • Schade: Arbeitsrecht, Kohlhammer 2010 • Martin T. Biegelman, Building World-Class Compliance Program: Best Practices and Strategies for Success, John Wiley & Sons; 2008. • Acquisti/ Gritzalis/Lambrinoudakis, Digital Privacy: Theory, Technologies, and Practices, Auerbach Pubn, 2007 • Sanjay Anand, Essentials of Sarbanes-Oxley, John Wiley & Sons, 2007. • CCH Incorporated, SEC Compliance and Disclosure Interpretations, Harcourt Professional Publishing, 2009. • Reyes, Carla, WTO-compliant Protection of Fundamental Rights: Lessons from the EU 'Privacy Directive, Melbourne Journal of International Law, Vol. 12, No. 1, Jun 2011: 141-176. • Spiros Simitis, Bundesdatenschutzgesetz, Nomos, Aufl. 7, 2011. • Aktuelle Gesetzestexte
Besonderes	Intensives Lesepensum

5. Organisatorische Aspekte des Sicherheitsmanagement

Modul-Kurzkennzeichen	SM_MA_OrgAsp_Sicherheitsmanagement
Modulbezeichnung	Organisatorische Aspekte des Sicherheitsmanagement
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
Autor/in	Prof. Dr. Ivo Keller
Dozent/in	Prof. Dr. Oliver Weissmann, Prof. Dr. Ivo Keller Holger Könnecke, Gerhard Reinhardt
Lehrsprache	Deutsch
Voraussetzungen	
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz- und 120 h Eigenstudium
Lehrform/SWS	Vorlesung: 2 x 15 Stunden, Bearbeitung von Fallbeispielen: 2 x 15 Stunden
Studien-/ Prüfungsleistungen	Praktische Arbeit + Referat und/oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote

Lernergebnisse	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Kennen der Prinzipien erfolgreicher Unternehmensführung • Beeinflussen von Unternehmenslenkern hin zur Beachtung von Sicherheitsaspekten und zum konstruktiven Umgang mit Krisensituationen • Ableiten einer Sicherheitsstrategie und von Sicherheitszielen aus der Unternehmensstrategie • Entwickeln einer Strategie zur Stärkung der ethischen Aspekte der Unternehmensführung • Lösen von Konflikten • Kennen der Methoden der Schutz- und Sicherheitstechnik • Analysieren der Einsatzmöglichkeiten und Wirkungsweisen von Schutzmechanismen gegen Elementarschäden, mechanischen Sicherheitseinrichtungen, Gefahrenmeldeanlagen und Beobachtungseinrichtungen • Planen eines Sicherheitssystemverbunds • Bewerten von am Markt angebotenen Lösungen • Einschätzen der rechtlichen Grundlagen für den Einsatz der einzelnen Sicherheitsmechanismen

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	• K. Macharzina: Unternehmensführung • T. Hutzschenreuther: Krisenmanagement • F. Glasl: Konfliktmanagement • B. Stackpole, E. Osendahl: Security Strategy: From Requirements to Reality. • Physical Security Systems Handbook von Michael Kairallah, 2005. • Aktuelle Journale und Zeitschriften zum Thema: kes, • Der Sicherheitsberater, S&I.
Besonderes	

6. Netzwerksicherheit

Modul-Kurzkennzeichen	SM_Ma_Netzwerksicherheit
Modulbezeichnung	Netzwerksicherheit
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
Autor/in	Prof. Dr. Eberhard von Faber
Dozent/in	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- und 120 h Eigenstudium
Lehrform/SWS	Vorlesung im Umfang von mindestens 30 Stunden sowie Übungen von bis zu 30 Stunden
Studien-/ Prüfungsleistungen	Praktische Arbeit + Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	• Kennenlernen der Bedrohungen und Herausforderungen in Netzwerken sowie wichtiger Gegenmaßnahmen in Form von Protokollen und diversen Sicherheitslösungen • Kennenlernen der Funktionsweise dieser Lösungen, Verständnis ihres Einsatzes, Betriebes und Zusammenwirkens; Fähigkeit, einige dieser Lösungen selbst zu integrieren und einzusetzen; Kennenlernen ergänzender Maßnahmen und Lösungen • Entwicklung der Fähigkeit, Anforderungen und industrielle Praxisfaktoren zu analysieren und Lösungen am praktischen Beispiel einer Branchenlösung zu integrieren • Kennenlernen von Sicherheitsmodulen und eingebetteten Systemen als Kernkomponenten für verteilte Systeme; Eigenschaften, Herausforderungen und Einsatz

Inhalte	• Erweiterte Grundlagen von Internet-Netzwerken (TCP/IP-Protokoll, ISO/OSI, Routing, aktive Komponenten, Kryptographie) • Gefahren beim Einsatz von IT, Kategorien von Bedrohungen, Schwachstellen und Gefährdungen • Sicherheitsmanagement, Sicherheitsaudits mit Tools, Netzwerkmonitoring und Netzwerklogging • Attacken und Gegenmaßnahmen • Kryptographieanwendungen (verschlüsselte Kommunikation, VPN-Protokolle, Zertifikate) • Web-Server-Sicherheit, E-Mail-Sicherheit • Vertiefung und praktische Anwendung in Projektthemen zu Firewalls, Honeypots und Intrusion-Detection-Systems, WLAN-Sicherheit und VPN
Lehr- und Lernmethoden	Kombination aus Vorlesung, Übungen am eigenen Computer und Übungen im Labor; Vorlesung mit gemischten Medien; Aufgaben und Übungsbeispiele; Kontrollfragen/Repetitorium
Literatur	• Cisco Networking Academy: CCNA Exploration Companion Guide, Bnd. 1-4, Cisco Press, 2008 • Alexander Michael: Netzwerke und Netzwerksicherheit - Das Lehrbuch, Hüthing Verlag, 2006. • Plötner Johannes, Wendzel Steffen: Praxishandbuch Netzwerk-Sicherheit, Galileo Computing, 2007. • Projektthemen (VPN, IPSec, IPv6, IDS, WLAN, Angriffe, u.a.m) Skripte und andere Lehrmaterialien werden während der Vorlesung direkt an die Studierenden verteilt bzw. stehen auf der Lernplattform der Hochschule zur Verfügung.
Besonderes	

7. Mathematisch-technische Grundlagen der IT-Sicherheit

Modul-Kurzkennzeichen	SM_MA_MathTechGrundlagen
Modulbezeichnung	Mathematisch-technische Grundlagen der IT-Sicherheit
ggf. Aufteilung in Lehrveranstaltungen	Grundlagen von Forensik und Auditing Grundlagen technischer Sicherheit
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
Autor/in	Prof. Dr. Friedrich Holl / Max Luber
Dozent/in	Prof. Dr. Igor Podebrad, Prof. Dr. Michael Syrjakow und ggf. weitere Dozenten des Studiengangs
Lehrsprache	Deutsch
Voraussetzungen	
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz- und 120 h Eigenstudium
Lehrform/SWS	Vorlesung: 2x 30 Stunden
Studien-/ Prüfungsleistungen	Grundlagen von Forensik und Auditing: Hausarbeit oder mündliche Prüfung Grundlagen technischer Sicherheit: Klausur oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	Das Ziel der Lehrveranstaltung „Grundlagen von Forensik und Auditing" ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Sichere Anwendung der mathematischen und technischen Grundlagen der Sicherheit, insbesondere • Organisieren von IT-forensischen Analysen und IT-Audits • Betreiben von IT-Systemen unter Berücksichtigung der Anforderungen an IT-Forensik und IT-Audit • Entwickeln und Durchsetzen von IT-Forensik-bezogenen Sicherheitsrichtlinien • Bewerten der Verwendbarkeit von IT-Audit-Ergebnissen für Forensik

	Das Ziel der Lehrveranstaltung „Grundlagen technischer Sicherheit " ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Symmetrische Verschlüsselung: informations-theoretisch sichere Verschlüsselung, klassische Verschlüsselungsverfahren, Blockchiffren (DES, AES), Stromchiffren, Verschlüsselungsmodi (z.B. CBC), Angriffe • Asymmetrische Verschlüsselung: RSA, Diffie-Hellman-Schlüsselaustausch, zahlentheoretische Grundlagen (Euklidischer Algorithmus, modulare Arithmetik, etc.), Angriffe • Nachrichtenauthentifizierung, digitale Signaturen, Public-Key-Infrastruktur (PKI), Angriffe • Aktuelle Trends in der Kryptographie (Quantenkryptographie, etc.)
Inhalte	• Gesetzliche Voraussetzungen für IT-Forensik • Prinzipien von IT-Audit • Organisation von IT-forensischen Analysen • Grundlagen kryptografischer Verfahren
Lehr- und Lernmethoden	Vorlesung und Übungen in Kleingruppen.
Literatur	• IT-Forensik von Alexander Geschonnek, 2011 • The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons, 2012 • Wolfgang Ertel: Angewandte Kryptographie; Fachbuchverlag Leipzig im Carl Hanser Verlag, 2003. • Klaus Schmeh: Kryptografie: Verfahren, Protokolle, Infrastrukturen; dpunkt Verlag, 2009.
Besonderes	Kryptographie: Verwendung des Werkzeugs „CrypTool“ zum Experimentieren mit kryptographischen Verfahren

8. Sichere IKT-Infrastrukturen und IT-Dienste

Modul-Kurzkennzeichen	SM_MA_SichereIKTInf_ITDienste
Modulbezeichnung	Sichere IKT-Infrastrukturen und IT-Dienste
ggf. Aufteilung in Lehrveranstaltungen	Sichere IKT-Infrastrukturen und IT-Dienste, Teil A WiSe Sichere IKT-Infrastrukturen und IT-Dienste, Teil B SoSe
Dauer des Moduls	Zweisemestrig
Zuordnung zum Curriculum	SM Ma, 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
Autor/in	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 zu Informations- und Kommunikationstechnologie: Anwendungen, Systeme und Netze sowie zugrundeliegende Technologien.
ECTS-Credits	6 gesamt; 2x 3 ECTS je Lehrveranstaltung
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz- und 120 h Eigenstudium
Lehrform/SWS	2 x 4 SWS in Blöcken von vier Lehrveranstaltungen je Semester; insgesamt 2x 30 Stunden. Vorlesung mit gemischten Medien, Angebot von Selbststudium und Hausaufgabe zur Vertiefung und Selbstkontrolle sowie Kontrollfragen/Repetitorium.
Studien-/ Prüfungsleistungen	Klausur oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	Gesamtnote Teil A und B: Je 50% der Fachnote; ca. 9% aller Fachnoten (6 von 69 ECTS); 6,25% der Abschlussnote

Lernergebnisse	Die Lernenden sollen in die Lage versetzt werden, die folgenden grundsätzlichen Kenntnisse und Fertigkeiten zu erlangen: Teil A: • Entwicklung der Fähigkeit, benötigte Lösungen adäquat in verschiedenen ITK-Infrastrukturen und Nutzungsszenarien zu integrieren; Kennenlernen von Dienstleistungsmodellen bis hin zum Cloud-Computing und deren Implikationen • Entwicklung der Fähigkeit, Anforderungen und industrielle Praxisfaktoren zu analysieren und Lösungen am praktischen Beispiel einer Branchenlösung zu integrieren • Erlernen von Grundlagen der Kryptografie und ihrer praktischen Anwendung sowie den Grenzen bzw. den Aufgaben für das Schlüsselmanagement • Verstehen, wie Anforderungen systematisch analysiert und umgesetzt werden; Entwicklung der Fähigkeit, selbst Sicherheit zu konzipieren und zu bewerten • Verstehen der Grundlagen von PKI als Beispiel einer Infrastruktur für die sichere Kommunikation • Prüfschemata als internationale Infrastruktur für das Risikomanagement verstehen und einordnen können Teil B: • Verstehen von Technik und Organisation moderner (industrieller) ITK-Produktion und speziell der auftretenden Sicherheitsfragen; Integration von Security-Management und IT-Service-Management • Verstehen der Sichtweisen Anwender und Produzent sowie von Grundlagen des Cloud-Computing; Nutzung und Einbindung von IT-Diensten in Geschäftsprozesse; Ermitteln von Sicherheitsanforderungen, Bewertung und Auswahl von IT-Diensten; Sicherheit und Vertrauenswürdigkeit • Erfolgreiches Einsetzen von Identitäts- und Zugriffs-management (IAM): Verstehen der Grundbegriffe, Architekturen und Technologien; Planung und Umsetzung in Unternehmen und in komplexen Wertschöpfungsketten
Inhalte	Teil A: • Integration der verschiedenen Lösungen im ITK-Verbund: Grundlegende Merkmale und Lösungen in den Bereichen: Traffic (Netze), Applications, Storage, Identities and Access, Data protection and privacy, Systems integrity, Intelligence and measurement und sonstiges; Architektur und Nutzungsszenarien: Absicherung durch adäquaten Einsatz verschiedenster Lösungen und Komponenten. • Lernbeispiel der speziellen Branchen-Anwendung „Bezahlsysteme": Anforderungen und Lösungen; Praxisfaktoren und Auswirkungen, industrielle Praxis • Grundlagen der Kryptografie: Typen kryptografischer Verfahren; Beispiele und Eigenschaften, Design-Prinzipien; Implementierung; Angriffe • Sicherheitsmodule und Schlüsselmanagement: Rolle und Notwendigkeit; Rolle der Kryptografie und ihre „Grenzen";

	Grundzüge des Schlüsselmanagements; Grundkonzept Personalisierung • Grundbegriffe der Informationssicherheit; Design-Ziele und Methoden zur Entwicklung adäquater Sicherheitsmaßnahmen • PKI: eine Infrastruktur für die sichere Kommunikation; Problemstellung; Lösungen; Zertifikate; Abläufe, Richtlinien und Standards • Assurance: eine Infrastruktur für „Vertrauen" und „Sicherheit" bei (globaler) Arbeitsteilung in industriellen Wertschöpfungsketten Teil B: • Anwender und Produzent: IT-Dienste; Sicherheitsanforderungen, Bewertung, Auswahl und Integration; Grund-probleme und „Sourcing"-Modelle einschl. Cloud; Sicherheits- und Risikomanagement beim „Outsourcing", Herausforderung für ICT-Service-Provider und Anwender(unternehmen) • Grundlagen der ITK-Produktion; ITK-Architekturen und Infrastrukturelemente; Sicherheitsaspekte; Management der Lösungen für die System- und Netzwerksicherheit; Prozesse und Organisation; Aufgaben vom Schwachstellenmanagement bis zum Disaster Recovery • Besonderheiten der industriellen ITK-Produktion; Probleme bei der Messbarkeit / Bewertung der Sicherheit; Integration von Security-Management und IT-Service-Management; Varianten der Strukturierung; Bedeutung von Architekturen und Ordnungsschemata mit Beispielen • Grundbegriffe IAM (alles von Identification bis Accounting), • Identitätsmanagement: Verwaltungsaufgaben, Registrierung, Workflows, Enrolment; Credential Management, User Self-Service, UHD etc. • Autorisierung (Access Management): Leistungen und Grenzen; Strategien (DAC, MAC, RBAC, IF); Realisierung (Gruppen, Rollen, ACL, Capabilities); Alternativen; Trends und Ausblick einschließlich DRM, • Authentisierung (Identity Verification): Arten, Methoden, Technologien; Probleme und Lösungen • Architekturen und IAM in verteilten Systemen (z.B. LDAP, RADIUS, Kerberos, Enterprise Single Sign-On (ESSO), Single Sign-On accross Web-Domains, Föderation von Web Services, Security Token Service, Active Directory) • Accounting; Analytics; Attestation; Intelligence; SOD • Aufsetzen und Durchführen von IAM-Programmen in Großunternehmen

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 • Common Criteria for Information Technology Security Evaluation; www.commoncriteriaportal.org oder ISO 15408 • Alexander Tsolkas und Klaus Schmidt: Rollen und Berechtigungskonzepte, Ansätze für das Identity- und Access Management im Unternehmen; August 2010, Vieweg+Teubner • Martin Kappes: Netzwerk- und Datensicherheit, Eine praktische Einführung; Vieweg+Teubner • Hans-Peter Königs: IT-Risiko-Management mit System, Von den Grundlagen bis zur Realisierung. Ein praxisorientierter Leitfaden, Vieweg • Claudia Eckert: IT-Sicherheit, Konzepte - Verfahren – Protokolle • Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond; Springer-Vieweg • Aktuelle Journale und Zeitschriften zum Thema: kes, Der Sicherheitsberater, S&I. Skripte und andere Lehrmaterialien werden während der Vorlesung direkt an die Studierenden verteilt.
Besonderes	

9. Secure Systems Lifecycle Management

Modul-Kurzkennzeichen	SM_MA_SecureSystems
Modulbezeichnung	Secure Systems Lifecycle Management
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 WI und Informatik Master angeboten werden.
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Ivo Keller
Dozent/in	Prof. Dr. Friedrich Holl, Sandro Hartenstein, Marcel Niefind
Lehrsprache	80% Deutsch, 20% 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 5.3: Dynamische Websites professionell programmieren von Christian Wenz und Tobias Hauser (Dezember 2009)
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz- und 120 h Eigenstudium
Lehrform/SWS	30 h Vorlesung, 30 h Übungen und gecoachte Selbstlernelemente
Studien-/ Prüfungsleistungen	Praktische Arbeit + Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote

Lernergebnisse	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: Kennen und Anwenden der vermittelten Best Practices während der Entwicklung von IT-basierten Systemen für sichere Software Entwickeln von Akzeptanzkriterien für nicht-funktionale Sicherheitsanforderungen Durchführen von Bedrohungsmodellierungen Vermeiden von Schwachstellen während der Entwicklung Durchführen von Sicherheitstests Sicheres Installieren und Betreiben von Software Etablieren eines Security Response Programms Analysieren von bestehender Software auf Sicherheitsschwachstellen Entwickeln und Umsetzen eines Schutzprogramms für Software während der Systementwicklung Etablieren eines Management-Systems für Sicherheit im Entwicklungsprozess, Integrieren dieses Management-Systems in einen eventuell vorhandenen Qualitätsprozess Durchführen von Sicherheitsanalysen („Hacking“) Darstellen von Untersuchungsergebnissen
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	Basiswissen sichere Software von Friedrich Holl, dpunkt 2011. Software-Qualität, Testen, Analysieren und Verifizieren von Software von Peter Liggesmeyer, Spektrum Akademischer Verlag, 2002. Writing Secure Code von Michael Howard & David LeBlanc, 2003 www.owasp.org
Besonderes	

10. Wissenschaftliches Schreiben

Modul-Kurzkennzeichen	SM_MA_WissSchreiben
Modulbezeichnung	Wissenschaftliches Schreiben
ggf. Aufteilung in Lehrveranstaltungen	Semesterarbeit 1 Semesterarbeit 2
Dauer des Moduls	Zweisemestrig
Zuordnung zum Curriculum	SecMan Master, 1. und 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls	
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Friedrich Holl
Dozent/in	Prof. Dr. Ivo Keller sowie alle anderen am Studiengang beteiligten Lehrenden
Lehrsprache	Deutsch
Voraussetzungen	
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 30 h Präsenz- und 150 h Eigenstudium
Lehrform/SWS	Vorlesung und Seminar mit Referat: 2 x 15 Stunden
Studien-/ Prüfungsleistungen	Schriftliche Arbeit
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	Erstellen von wissenschaftlichen Arbeiten unter Anleitung im Themenfeld der Sicherheit
Inhalte	Erhebungsmethoden (Statistik, Interview, primär/sekundär Quellen) Quellendiskussion: recherchieren, lesen, bewerten Kreativtechniken und Selbstorganisation situationsbezogene Anforderungen an Schreibstile (Werbung, Pressemitteilung, wiss. Arbeit …) Erstellung eines Exposés Methodischer Aufbau wiss. Arbeiten Phasen des wissenschaftlichen Arbeitens Materialsammlung und Recherche Materialbewertung und -Auswahl Material- und Themenbearbeitung Zitiersysteme
Lehr- und Lernmethoden	Vorlesung, Diskussion, Vorstellen der eigenen Ergebnisse.

Literatur	DIN 1421 (Gliederung und Benummerung in Texten) Eco, U. (2005) Wie man eine wissenschaftliche Abschlussarbeit schreibt - Doktor-, Diplom- und Magisterarbeit in den Geistes- und Sozialwissenschaften, Müller, Heidelberg, Theisen, Manuel R.: Wissenschaftliches Arbeiten - Technik Methodik, Form, 2000. Peterßen, Wilhelm H.: Wissenschaftliche(s) Arbeiten - Eine Einführung für Schule und Studium, 1999.
Besonderes	

11. Projekt

Modul-Kurzkennzeichen:	SM_MA_Projekt
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
Autor/in:	Prof. Dr. Friedrich Holl
Dozent/in:	Prof. Dr. Friedrich Holl sowie alle anderen am Studiengang beteiligten Lehrenden
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz- und 120 h Eigenstudium
Lehrform/SWS:	Vorlesung: 15 Stunden Nachweis von praktischem Arbeiten: 45 Stunden
Studien-/ Prüfungsleistungen:	Praktische Arbeit + Referat
Gewichtung der Note in der Gesamtnote:	6,25% der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: - Durchführen von Sicherheitsprojekten - Planen eines sicherheitsbezogenen Projekts unter ganzheitlicher Beachtung der Anforderungen - Anwenden von Projektmanagement-Methodiken

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 Delphimethode, Erarbeitung der Kontextes über Dokumente usw. Sollkonzeptentwicklung: - wissenschaftlich fundierte Entwicklung eines praxisorientierten Lösungsansatzes - Nutzung von Kreativmethoden - Kosten- Nutzen – Analysen - Entwicklung von Rahmenbedingungen des Einsatzes Prototypische Umsetzung - die prototypische Umsetzung erfolgt durch Entwicklung eines Software-Prototypen - Umsetzung im Unternehmen/ Organisation oder Entwicklung bspw. eines Antrags auf Forschungs- und Entwicklungsförderung
Lehr- und Lernmethoden:	Vorlesung, praktisches Arbeiten in Gruppen bis maximal 7 Teilnehmer, Vorstellen der eigenen Ergebnisse.
Literatur:	A Guide to the Project Management Body of Knowledge, PMI, 2008
Besonderes:	Die Bereitschaft zu praktischem Arbeiten bei Kooperationspartnern wird vorausgesetzt.

12. Masterarbeit

Modul-Kurzkennzeichen	Masterarbeit
Modulbezeichnung	Masterarbeit incl. Masterseminar
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
Autor/in	Prof. Dr. Friedrich Holl
Dozent/in	Der Erstgutachter einer Master-Arbeit muss ein Professor der Technische Hochschule Brandenburg sein. Der Zweitgutachter wird in Abstimmung mit dem Erstgutachter ausgewählt
Lehrsprache	Deutsch / Englisch (Wahl des Studenten).
Voraussetzungen	Zur Master-Arbeit kann sich nur anmelden, wer alle Prüfungsleistungen bis auf die Wahlpflichtmodule erfolgreich absolviert hat.
ECTS-Credits	21
Gesamtworkload und ihre Zusammensetzung	600h Selbststudium
Lehrform/SWS	Selbststudium.
Studien-/ Prüfungsleistungen	Master-Arbeit (87,5%) Kolloquium (12,5%)
Gewichtung der Note in der Gesamtnote	30% der Abschlussnote
Lernergebnisse	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: Erstellen einer wissenschaftlichen Arbeit unter Anleitung mit eigenen kreativen und/oder konstruktiven Anteilen im Themenfeld des „Security Management" in einem Zeitraum von 4 Monaten (in Teilzeit 8 Monate). 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 a. (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: ein Leitfaden für Haus-, Seminar- und Diplomarbeiten sowie Dissertationen. Wien Pyrczak, S. et. Al. (1998). Writing empirical Research Reports. Los Angeles. C.A. Seale, C. (1999). The quality of quantitative research. London Trachim, W. M. K. (2000). The Research Knowledge Base. Cincinatti. Ohio
Besonderes	