



---

# Modulkatalog des Master-Studiengangs Security Management

---

## Inhaltsverzeichnis:

<b>1</b>	<b>Security Management</b> .....	<b>3</b>
1.1	Grundlagen des Security Management.....	3
1.2	Security- und Krisenmanagement im internationalen Kontext .....	5
1.3	Gebäude- und Arbeitsplatzsicherheitsmanagement .....	6
<b>2</b>	<b>IT-Sicherheit</b> .....	<b>8</b>
2.1	Netzwerksicherheit .....	8
2.2	Netzwerksicherheitsmanagement .....	10
2.3	Entwicklung sicherer IT-Systeme .....	12
<b>3</b>	<b>Mathematische und physikalische Grundlagen</b> .....	<b>14</b>
3.1	Grundlagen sicherer Kommunikationstechnik .....	14
3.2	Kryptologie.....	16
<b>4</b>	<b>Recht und Betriebswirtschaftslehre</b> .....	<b>18</b>
4.1	Recht.....	18
4.2	Unternehmensführung, Personal- und Konfliktmanagement.....	21
<b>5</b>	<b>Sonstige Studienleistungen</b> .....	<b>23</b>
5.1	Semesterarbeit 1 und 2 .....	23
<b>6</b>	<b>Wahlpflicht und Projekte</b> .....	<b>25</b>
6.1	Projekt.....	25
6.2	Wahlpflichtfächer 1, 2 und 3 .....	28
<b>7</b>	<b>Masterseminar / Masterarbeit mit Kolloquium</b> .....	<b>30</b>



# 1 Security Management

## 1.1 Grundlagen des Security Management

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Grundlagen des Security Management
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Überblick, Einblick und erste Erfahrungen in Unternehmenssicherheit. Erstellen von Business Cases zu Sicherheitsthemen. Risikoeinschätzung und Abwägen von Bedrohungen, Wirksamkeit von Massnahmen und Kosten. Verständnis für die Rolle des "Trusted Advisor" im eigenen Unternehmen
Inhalt der Lehrveranstaltung	Was ist Sicherheit –Technik und Verhalten –Psychologie und Sicherheit (Awareness) –SecurityPolicy –Risiko-management – SecurityManagement als Prozess – SecurityGovernance - Incidents, Krisen und Katastrophen – Incident Management –Krisenmanagement und Business Continuity–SecurityReporting – SecurityPortfolio Management –Rolle der Security-Abteilung–Anforderungen an die Mitarbeiter –Erfolgskriterien für Security Management Im weiteren beispielhaft: Identitätsmanagement – Information Management –Sicherheitsarchitektur –Business Continuityam Beispiel der Vogelgrippe –Anwendung von Standards –Beziehungen zu Lieferanten und Kunden – Physische Sicherheit –CERT-Betrieb–ERP- Sicherheit – Sichere Software-Entwicklung –Personen-und Abhörschutz
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	1. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	6 ( Workload: 180 Stunden = 65 h Präsenz- und 115 h Eigenstudium)
Verantwortliche	Prof. Dr. Sachar Paulus
Lehrende	Prof. Dr. Sachar Paulus; Prof. Dr. Friedrich-L. Holl
Prüfungsform	Sonstige schriftliche Arbeit + Referat u./o. mündl. Prüfung
Zugangsvoraussetzungen	allgemeine Kenntnisse der Betriebswirtschaft sind hilfreich
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	Klaus-Rainer Müller: Handbuch Unternehmenssicherheit, Vieweg, Wiesbaden, 2005
Lehr- und Lernmethoden	Vorlesung mit gemischten Medien (Beamer und Tafel), Erarbeiten von Einsichten in Kleingruppen, Mini-Projekte (3 Personen) über mehrere Stunden, Rollenspiele, Individuelle Präsentation.
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Präsentation und Abschlussbericht, Präsentation eines Business Case Proposals, 20 min mit anschließender Verteidigung der Argumentation + schriftliche Ausarbeitung desselben.
Unterrichts-/Lehrsprache	Deutsch

Besonderes (z.B. Online-Anteil, Praxisbesuche, Gast sprecher etc.)	Sehr viel Gruppendynamik.
---	---------------------------

## 1.2 Security- und Krisenmanagement im internationalen Kontext

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Security- und Krisenmanagement im internationalen Kontext
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Vertiefung der in Grundlagen des Security Management erworbenen Kenntnisse, insbesondere Anwendung auf praxisnahe Situationen mit hohem persönlichem Druck
Inhalt der Lehrveranstaltung	Sicherheitsmanagement in globalen Organisationen Kommunikationsaspekte zwischen Sicherheits-Teams, Klärung von Verantwortlichkeiten Krisenmanagement: Krisen praktisch bewältigen Krisenkommunikation: Prinzipien und Vorgehensweisen bei der Kommunikation in Krisenfällen Individuelle Kompetenzen für Sicherheits- und Krisenmanagement, z.B. für Telefonzentralen Auswirkung von Sicherheit Erstellen einer öffentlichkeitswirksamen Kampagne für Sicherheitsthemen
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	2. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	6 ( Workload: 180 Stunden = 65 h Präsenz- und 115 h Eigenstudium)
Verantwortliche	Prof. Dr. Sachar Paulus
Lehrende	Prof. Dr. Sachar Paulus; Prof. Dr. Friedrich-L. Holl
Prüfungsform	Sonstige schriftliche Arbeit + Referat u./o. mündl. Prüfung
Zugangsvoraussetzungen	Grundlagen des Security Management
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	wird bekannt gegeben
Lehr- und Lernmethoden	Vorlesung mit gemischten Medien (Beamer und Tafel), Erarbeiten von Einsichten in Kleingruppen, Mini-Projekte (3 Personen) über mehrere Stunden, Rollenspiele, Individuelle Präsentation.
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Präsentation mit Rollenspiel, Erarbeitung es Gesamtkonzepts und Vorstellung. Abschlussbericht.
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	Sehr viel Gruppendynamik.

### 1.3 Gebäude- und Arbeitsplatzsicherheitsmanagement

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Gebäude- und Arbeitsplatzsicherheitsmanagement
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	<p>Im Fach „Gebäude- und Arbeitsplatzsicherheitsmanagement“ werden die Studierenden mit methodischen und technischen Grundlagen der Schutz- und Sicherheitstechnik vertraut gemacht.</p> <p>Die inhaltlichen Schwerpunkte der Lehrveranstaltung liegen daher bei Einsatzmöglichkeiten und Wirkungsweise von Schutzmechanismen gegen Elementarschäden, mechanischen Sicherheitseinrichtungen, Gefahrenmeldeanlagen und Beobachtungseinrichtungen.</p> <p>Die Studierenden erhalten einen umfassenden Einblick in derzeit am Markt erhältliche Sicherheitssysteme und lernen deren Funktionsweise sowie mögliche Anwendungsgebiete und sicherheitstechnische Grenzen der Systeme kennen.</p> <p>Großer Wert wird auch auf die Auseinandersetzung mit den rechtlichen Rahmenbedingungen für den Einsatz der einzelnen Sicherheitsmechanismen gelegt.</p>
Inhalt der Lehrveranstaltung	<ul style="list-style-type: none"> <li>• Grundlagen der Gebäude- und Arbeitsplatzsicherheit <ul style="list-style-type: none"> <li>- Begriffe und Überblick über Aufgabengebiete und Möglichkeiten</li> <li>- technische Grundlagen</li> </ul> </li> <li>• physische Angriffe und ihre Wirkung <ul style="list-style-type: none"> <li>- Elementarschäden</li> <li>- Angreifer, Ziele und Angriffsmethoden</li> <li>- Waffen und ihre Wirkung</li> <li>- Abstrahlung elektronischer Geräte</li> </ul> </li> <li>• Mechanische Sicherheitseinrichtungen und Zutrittskontrolle <ul style="list-style-type: none"> <li>- Schlösser, Schließanlagen und ihre Sicherheit</li> <li>- Angriffssicherung an Türen und Fenstern und Zaunanlagen</li> <li>- Wertbehältnisse und Datensicherungsschränke</li> <li>- technische und rechtliche Vorschriften und Richtlinien</li> </ul> </li> <li>• Gefahrenmeldeanlagen <ul style="list-style-type: none"> <li>- Grundlagen</li> <li>- Einbruchmeldeanlagen</li> <li>- Überfallmeldeanlagen</li> <li>- technische Störungsmeldeanlagen</li> <li>- Brandmelde- und Brandbekämpfungsanlagen</li> <li>- technische und rechtliche Vorschriften und Richtlinien</li> </ul> </li> <li>• Beobachtungseinrichtungen <ul style="list-style-type: none"> <li>- technische Möglichkeiten</li> <li>- offene und verdeckte Überwachung</li> <li>- technische und rechtliche Vorschriften und Richtlinien</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Notfallplanung und betriebliche Sicherheit <ul style="list-style-type: none"> <li>- Folgeschädenanalyse</li> <li>- Handhabung von Vorfällen</li> </ul> </li> </ul>
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	2. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	3 ( Workload: 90 Stunden = 30 h Präsenz- und 60 h Eigenstudium)
Verantwortliche	Ralph Wölpert
Lehrende	Ralph Wölpert, Thorsten Weller, Ralf Dahmer, Thomas Koch
Prüfungsform	Klausur, u./o. mündl. Prüfung
Zugangsvoraussetzungen	
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	Zeitschriften: kes, IT-Management, IT-Director, LANline, Der Sicherheitsberater, S&I,
Lehr- und Lernmethoden	Vorlesung mit gemischten Medien (Beamer und Folien), Übung im PC-Hörsaal in kleinen Gruppen (bis 10 Personen)
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Fragen/Antworten während der Vorlesung, Vorbereitung auf die Prüfung mittels Beispielfragen, Prüfung: 10 Fragen, ausführliche Textantworten, 60 min.
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	

## 2 IT-Sicherheit

### 2.1 Netzwerksicherheit

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Netzwerksicherheit
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Die Lehrveranstaltung vermittelt ein übergreifendes praktisches Verständnis von der Sicherheit in IP-basierten Kommunikationsnetzen. Analysiert werden die Risiken und Gefahren, die mit der Ausnutzung von Schwachstellen in Protokollen und Anwendungen, oberflächlicher Installationen und fehlender Sicherheits-Policies in Unternehmen einhergehen. Die Studenten lernen an praktischen Beispielen den Ablauf und die Strategie von Angriffen kennen und leiten daraus Maßnahmen für einen sicheren Betrieb von Netzwerkkomponenten ab.
Inhalt der Lehrveranstaltung	<ul style="list-style-type: none"> <li>- Erweiterte Grundlagen von Internet-Netzwerken (TCP/IP-Protokoll, ISO/OSI, Routing, aktive Komponenten, Kryptographie)</li> <li>- Gefahren beim Einsatz von IT, Kategorien von Bedrohungen, Schwachstellen und Gefährdungen</li> <li>- Sicherheitsmanagement, Sicherheitsaudits mit Tools, Netzwerkmonitoring und Netzwerklogging</li> <li>- Attacken und Gegenmaßnahmen</li> <li>- Kryptographieanwendungen (verschlüsselte Kommunikation, VPN-Protokolle, Zertifikate)</li> <li>- WEB-Server-Sicherheit, E-Mail-Sicherheit</li> <li>- Vertiefung und praktische Anwendung in Projektthemen zu Firewalls, Honneypots und Intrusion-Detection-Systeme, WLAN-Sicherheit und VPNs</li> </ul>
Code der Lehrveranstaltung	
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	1. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	6 ( Workload: 180 Stunden = 65 h Präsenz- und 115 h Eigenstudium)
Verantwortliche	Dietmar Hausmann
Lehrende	Dietmar Hausmann; E. v. Faber
Prüfungsform	Projektarbeit + Referat u./o. mündl. Prüfung
Zugangsvoraussetzungen	Kenntnisse zu den Grundlagen von Internet-Netzwerken, Betriebssystemen und kryptographiebasierten Techniken werden vorausgesetzt.
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	Alexander Michael: Netzwerke und Netzwerksicherheit - Das Lehrbuch, Hüthing Verlag, 2006. Plötner Johannes, Wendzel Steffen: Praxishandbuch Netzwerk-Sicherheit, Galileo Computing, 2005.

	<p>Wätjen Dietmar: Kryptographie. Grundlagen, Algorithmen, Lehrbuch Protokolle, Spektrum Akademischer Verlag, 2004.</p> <p>Peikari, Cyrus and Chuvakin, Anton: Kenne deinen Feind - Fortgeschrittene Sicherheitstechniken, O'Reilly Verlag, 2004.</p> <p>Scambray Joel, McClure Stuart, Kurtz George - Das Anti-Hacker-Buch, mitp Verlag, 2004.</p> <p>Vertiefende Literatur zu speziellen Themen (VPN, IPSEC, IDS, Firewalls)</p> <p>Elektronischer Zugriff auf Lehrscripte über den BSCW-Server des Fachbereichs</p>
Lehr- und Lernmethoden	Vorlesung, Übung zu konkreten Fragestellungen aus der Vorlesung
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Projektarbeit mit Referat Die jeweilige Projektarbeit wird praxisnah formuliert und soll in eine produktive Lösung integriert werden können.
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	

## 2.2 Netzwerksicherheitsmanagement

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Netzwerksicherheitsmanagement
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	<p>In Anlehnung an die Lehrveranstaltung „Netzwerksicherheit“ werden in „Netzwerksicherheitsmanagement“ Methoden- und Fachkompetenz in Bezug auf den Aufbau und die Ausgestaltung von IT-Sicherheitsinfrastrukturen vermittelt. Die Studierenden werden sich kritisch mit den aus „Netzwerksicherheit I“ bekannten Angriffsmustern und Schutzmechanismen auseinandersetzen und ein tiefgreifendes Verständnis für grundlegende Probleme der betrieblichen IT-Sicherheit entwickeln.</p> <p>Sie werden sowohl managementorientiertes Wissen zu Sicherheitsmodellen und Sicherheitspolitiken als auch technische Kompetenz im Bereich von Problemfeldern wie dem Schlüsselmanagement, der Computerforensik und der Evaluation von IT-Sicherheitssystemen erwerben.</p>
Inhalt der Lehrveranstaltung	<ul style="list-style-type: none"> <li>• Datensicherheit</li> <li>• Archivierungssysteme</li> <li>• Disaster Recovery</li> <li>• Sicherheitsmodelle <ul style="list-style-type: none"> <li>- Modellklassifikation</li> <li>- Zugriffskontrollmodelle und Informationsflussmodelle</li> <li>- Einsatzrichtlinien</li> </ul> </li> <li>• Schlüsselmanagement in Netzwerkinfrastrukturen <ul style="list-style-type: none"> <li>- Zertifikate, Zertifizierung, Zertifizierungsstellen und PKI</li> <li>- Schlüsselerzeugung, -aufbewahrung und -zerstörung, Schlüsselerückgewinnung</li> <li>- Schlüsselverteilung</li> </ul> </li> <li>• Sicherheitspolitiken und deren Um- und Durchsetzung, benutzergerechte Gestaltung von Sicherheitsmechanismen</li> <li>• Intrusion Detection and Prevention</li> <li>• Computerforensik</li> <li>• Trusted Computing und Digital Rights Management</li> <li>• Evaluation von IT-Sicherheitssystemen <ul style="list-style-type: none"> <li>- Bewertungskriterien für IT-Systeme und Infrastrukturen</li> <li>- Grundschutz</li> <li>- Common Criteria</li> </ul> </li> </ul>
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	2. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	3 ( Workload: 90 Stunden = 30 h Präsenz- und 60 h Eigenstudium)

Verantwortliche	Dr. Eberhard von Faber
Lehrende	Dr. Eberhard von Faber
Prüfungsform	Projektarbeit + Referat u./o. mündl. Prüfung
Zugangsvoraussetzungen	Anwendbare Kenntnisse zu Netzwerken, Betriebssystemen und kryptographiebasierten Techniken werden vorausgesetzt. Grundkenntnisse Geschäftsprozesse und Unternehmensorganisation; Grundkenntnisse Informationstechnologie: Anwendungen, Systeme und Netze sowie zugrundeliegende Technologien.
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	Alexander Michael: Netzwerke und Netzwerksicherheit - Das Lehrbuch, Hüthing Verlag, 2006. Plötner Johannes, Wendzel Steffen: Praxishandbuch Netzwerk-Sicherheit, Galileo Computing, 2005. Wätjen Dietmar: Kryptographie. Grundlagen, Algorithmen, Lehrbuch Protokolle, Spektrum Akademischer Verlag, 2004. Peikari, Cyrus and Chuvakin, Anton: Kenne deinen Feind - Fortgeschrittene Sicherheitstechniken, O'Reilly Verlag, 2004. Scambray Joel, McClure Stuart, Kurtz George - Das Anti-Hacker-Buch, mitp Verlag, 2004. Vertiefende Literatur zu speziellen Themen (VPN, IPSEC, IDS, Firewalls) Elektronischer Zugriff auf Lehrscripte über den BSCW-Server des Fachbereichs
Lehr- und Lernmethoden	Vorlesung mit gemischten Medien (Beamer und Folien), Übung im PC-Hörsaal in kleinen Gruppen (bis 10 Personen) Vorlesung, Übung zu konkreten Fragestellungen aus der Vorlesung, Zur Durchführung der Übungen steht ein separates Labor zur Verfügung. Die jeweiligen Fall- und Projektbeispiele werden innerhalb der Lehrveranstaltung erarbeitet.
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Projektarbeit mit Referat Die jeweilige Projektarbeit wird praxisnah formuliert und soll in eine produktive Lösung integriert werden können.
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	

### 2.3 Entwicklung sicherer IT-Systeme

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Entwicklung sicherer IT-Systeme
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	<p>Ausgehend von Grundlagenkenntnissen, die den Studierenden aus den Lehrveranstaltungen Netzwerksicherheit und Kryptologie bekannt sind, führt die Lehrveranstaltung „Entwicklung sicherer Systeme“ die Studierenden in die neue Ingenieursdisziplin „Security Engineering“ ein.</p> <p>Vermittelt werden hierbei Techniken zur Erfassung relevanter Systemeigenschaften, die Anwendung von Schutzbedarfsfeststellung, Bedrohungs- und Risikoanalyse beim Entwurf von IT-Systemen sowie die Erstellung und Umsetzung von Sicherheitsstrategien und Sicherheitsarchitekturen anhand allgemein verbreiteter Phasenmodelle der Systemkonstruktion.</p> <p>Des Weiteren werden Techniken und Werkzeuge zur Entwicklung von Software für den Einsatz in kritischen Anwendungsbereichen vorgestellt und deren Möglichkeiten und Grenzen erprobt.</p> <p>Die Studierenden erhalten damit einen umfassenden und praxisnahen Einblick in moderne Methoden des Designs von sicherheitskritischen IT-Anwendungen und qualifizieren sich damit für eine berufliche oder wissenschaftliche Weiterbeschäftigung mit diesem hochgradig komplexen Teil der IT-Sicherheit.</p>
Inhalt der Lehrveranstaltung	<ul style="list-style-type: none"> <li>• Software-Engineering, Programmierung und Hardware-Design</li> <li>• Security-Engineering <ul style="list-style-type: none"> <li>- Entwicklungsprozess, Phasenmodelle und Konstruktionsprinzipien</li> <li>- Strukturanalyse und Schutzbedarfsermittlung</li> <li>- Risikoanalyse</li> <li>- Sicherheitsstrategie, Sicherheitsarchitektur und Validierung</li> </ul> </li> <li>• Sicherheitsaspekte bei der Implementierung von IT-Systemen <ul style="list-style-type: none"> <li>- Programmierfehler als Sicherheitsrisiken</li> <li>- Sicherheitsaspekte bei der Programmierung</li> <li>- Programmiersprachen und Betriebssysteme</li> <li>- Entwicklungswerkzeuge</li> <li>- benutzergerechte Gestaltung interaktiver IT-Sicherheitssysteme, Mensch-Computer-Interaktion</li> </ul> </li> <li>• Evaluation von IT-Sicherheitssystemen <ul style="list-style-type: none"> <li>- Testverfahren und Vorgehensweisen, z.B. Junit</li> <li>- semiformale und formale Verifikation von IT-Systemen</li> </ul> </li> </ul>
Art der Lehrveranstaltung	Pflicht

(Pflicht, Wahl, etc.)	
Semester/Trimester	2. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	6 ( Workload: 180 Stunden = 65 h Präsenz- und 115 h Eigenstudium)
Verantwortliche	Prof. Dr. Thomas Schwotzer
Lehrende	Prof. Dr. Thomas Schwotzer; Prof. Dr. Michael Syrjakow; Prof. Dr. Schmidt
Prüfungsform	Projektarbeit + Referat o. Klausur u./o. mündl. Prüfung
Zugangsvoraussetzungen	Grundlagenkenntnisse im Software Engineering: objektorientierte Modellierung und Programmierung
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	N. Leveson: Safeware: System Safety and Computers, Addison-Wesley Longman, Amsterdam, 1995.  S. J. Powell, R. C. Linger, J. H. Poore: Cleanroom Software Engineering: Technology and Process, Addison-Wesley Professional, 1999.  G. J. Myers: Methodisches Testen von Programmen, Oldenbourg, Auflage: 7., Aufl., 2001  Peter Liggesmeyer: Software-Qualität, Testen, Analysieren und Verifizieren von Software, Spektrum Akademischer Verlag, 2002.  Andrew Hunt, David Thomas: Pragmatisch Programmieren Uni-Tests mit Junit, Hanser Fachbuchverlag; Auflage: 1, 2005.  Elfriede Dustin, Jeff Rashka, John Paul: Software Automatisch Testen, Springer, Berlin, 1. Aufl., 2001.
Lehr- und Lernmethoden	Vorlesung mit gemischten Medien (Beamer und Folien), Übung im PC-Hörsaal in kleinen Gruppen (bis 10 Personen)
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Praktische Arbeit: Erfolgreicher Entwicklung eines sicheren Softwaresystems Bestehen einer Abschlussklausur/mündl. Prüfung, benotet Die Note entspricht der Note der praktischen Arbeit und der Abschlussklausur
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	

### 3 Mathematische und physikalische Grundlagen

#### 3.1 Grundlagen sicherer Kommunikationstechnik

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Grundlagen der sicheren Kommunikationstechnik
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Ausstattung mit dem Rüstzeug eines Security-Analytikers/Designers; stetiges Denken in Angriff und Verteidigung; Nutzen von Analogien und Modellen; Denken in Szenarien; Entwicklung der Fähigkeit, selbst Sicherheit zu konzipieren/zu bewerten; Konzept „tamper-proof“ und dessen Realisierung; Kennenlernen Hardware naher Sicherheitsmaßnahmen und spezifischer Angriffsmethoden
Inhalt der Lehrveranstaltung	Bezahlsysteme: Abbildung von Interaktionen auf elektronische Vorgänge, Notwendigkeit von Sicherheitsmodulen (z.B. als Schlüsselspeicher); Möglichkeiten und Grenzen der elektronischen Kommunikation, Schlüsselmanagement, Prozesse und Systeme; grundlegende Bedrohungsmodelle mit indirekten/direkten Angriffen und Covered-Channels; logische versus physikalische Sicherheit, Grundkonzepte und Design-Kriterien; Embedded Systems: Bedrohungsmodell; Sicherheitselemente und -mechanismen; Lebenszyklus und Device-Management; Chipkarten: Arten/Typen/Eigenschaften, Lebenszyklus; Produktionsprozesse einschließlich Personalisierung; Wie funktioniert ein „Computer“?, Chipkarten: Architektur, Programmierung und Realisierung; Bedrohungs- und Angriffsmodell; Angriffsmethoden wie DFA, DPA, reverse-engineering, chip manipulation u.a.; Tools und Techniken; Sicherheitsmechanismen und deren Überwindung in der Praxis; Konzept Vertrauenswürdigkeit.
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	1. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	3 ( Workload: 90 Stunden = 30 h Präsenz- und 60 h Eigenstudium)
Verantwortliche	Dr. Eberhard von Faber
Lehrende	Dr. Eberhard von Faber
Prüfungsform	Klausur; u./o. mündl. Prüfung
Zugangsvoraussetzungen	Bedeutung der IT-Sicherheit und deren Rolle in der Praxis; technische und physikalische Grundkenntnisse; weitere Grundlagen werden parallel in der LV „Kryptologie“ vermittelt
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	[1] Anderson, Ross: Security Engineering, A Guide to Building Dependable Distributed Systems; John Wiley & Sons, Inc.; 2001 [2] FIPS PUB 140-2, Security Requirements for Cryptographic Modules; National Institute of Standards and Technology; 2002; <a href="http://csrc.nist.gov/cryptval/">http://csrc.nist.gov/cryptval/</a> [3] Common Criteria for Information Technology Security

	<p>Evaluation (auch ISO15408), Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements  <a href="http://www.bsi.de/cc/index.htm">http://www.bsi.de/cc/index.htm</a> oder  <a href="http://www.commoncriteriaportal.org">http://www.commoncriteriaportal.org</a> (sowie: CEM)</p> <p>[4] BSI-PP-0002, Smartcard Integrated Circuit Platform Protection Profile; Version 1.0, Juli 2001 (E. von Faber main technical editor); Smartcard Integrated Circuit Augmentations; Version 1.0, March 2002;  <a href="http://www.bsi.bund.de/cc/pplist/pplist.htm">http://www.bsi.bund.de/cc/pplist/pplist.htm</a></p> <p>[5] Rankl, Wolfgang und Effing, Wolfgang: Handbuch der Chipkarten, Aufbau, Funktionsweise, Einsatz von Smart Cards; Hanser Fachbuchverlag, 2002</p> <p>Skripte und andere Lehrmaterialien werden während der Vorlesung direkt an die Studierenden verteilt</p>
Lehr- und Lernmethoden	Vorlesung mit gemischten Medien (Beamer und Folien), Übung im PC-Hörsaal in kleinen Gruppen (bis 10 Personen)
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Klausur; benotet, 90 Minuten; bei wenigen Teilnehmern oder verbesserungswürdigen Ergebnissen mündliche Prüfung; Prüfungsfach im Verbund mit der LV Kryptologie
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gast sprecher etc.)	

### 3.2 *Kryptologie*

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Kryptologie
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Die Lehrveranstaltung Kryptologie soll den Studierenden Kenntnissein Bezug auf die mathematischen Grundlagen der sicheren Informationsübertragung vermitteln. In diesem Sinne befasst sich die Lehrveranstaltung sowohl mit der Informationstheorie, primär jedoch mit der Kryptographie und Kryptoanalyse.
Inhalt der Lehrveranstaltung	<p>Die Studierenden sollen mit den Methoden der Geheimhaltung, der Integritätssicherung und der Authentizitätssicherung im elektronischen Nachrichtenverkehr vertraut gemacht werden, ein tiefgreifendes Verständnis für gebräuchliche kryptographische Protokolle entwickeln und deren Stärken und Schwächen einzuschätzen lernen. Ein Schwerpunkt liegt dabei in Methoden zur Ermöglichung eines sicheren elektronischen Geschäftsverkehrs.</p> <p>Im Rahmen der Übungen werden die Studierenden den Umgang mit kryptographischen Anwendungen erproben, Details zur Implementierung der Verfahren erfahren und sich mit Methoden der Kryptoanalyse vertraut machen. Ferner wird von ihnen erwartet, eine ca. zwanzigseitige Semesterarbeit zu einem speziellen Thema aus dem Bereich der Kryptologie zu erstellen und damit sowohl fachliche Kenntnisse als auch die Fähigkeit zur kritischen Auseinandersetzung mit dem Thema und zum wissenschaftlichen Arbeiten nachzuweisen.</p>
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	1. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	3 ( Workload: 90 Stunden = 30 h Präsenz- und 60 h Eigenstudium)
Verantwortliche	Prof. Dr. Michael Syrjakow
Lehrende	Prof. Dr. Michael Syrjakow
Prüfungsform	Klausur; u./o. mündl. Prüfung
Zugangsvoraussetzungen	
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	<p>Beutelspacher, Kryptologie, Vieweg, 2005</p> <p>J. Daemen – V. Rijmen, The Design of Rijndael.AES, Springer, 2001</p> <p>C. A. Deavours – L. Kruh, Machine Cryptography and Modern Cryptanalysis, Artech House Publishers, 1985</p> <p>D. E. Knuth, The Art of Computer Programming 2, Seminumerical Algorithms, Addison-Wesley, 1998</p>

	<p>A. J. Menezes - P. van Oorschoot - S. Vanstone, Handbook of Applied Cryptography, CRC, 1996</p> <p>M. Rosing, Implementing Elliptic Curve Cryptography, Manning Publications, 1998</p> <p>B. Schneier, Angewandte Kryptographie, Pearson Studium, 2005</p> <p>A. Sinkov, Elementary Cryptanalysis, The Mathematical Association of America, 1998</p> <p>M. Welschenbach, Cryptography in C and C++, Apress, 2005</p> <p>J. Bamford, Body of Secret: Anatomy of the Ultra-Secret National Security Agency, Anchor, Reprint Edition, 2002</p>
Lehr- und Lernmethoden	Vorlesung mit gemischten Medien (Beamer und Folien), Übung im PC-Hörsaal in kleinen Gruppen (bis 10 Personen)
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Klausur; benotet, 90 Minuten; bei wenigen Teilnehmern oder verbesserungswürdigen Ergebnissen mündliche Prüfung; Prüfungsfach im Verbund mit der LV „Grundlagen der sicheren Kommunikationstechnik“
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	Einsatz des E-Learning-Programms CrypTool <a href="http://www.cryptool.de/">http://www.cryptool.de/</a>

## 4 Recht und Betriebswirtschaftslehre

### 4.1 *Recht*

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Recht
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Rahmenbedingungen von Sicherheitsmaßnahmen
Inhalt der Lehrveranstaltung	<p><b>1. Haftungsrecht, Insolvenzrecht</b> Vertragliche Grundlagen, Verschuldens- und Gefährdungshaftung, Deliktsrecht, Voraussetzungen und Ablauf (Unternehmens-, Verbraucherinsolvenzverfahren und Restschuldbefreiungsverfahren)</p> <p><b>2. Telekommunikationsrecht</b> Systematik und Inhalt im TKG, Richtlinien 2001/21/EG; 2002/19/EG, 2002/22/EG, TKV, TKÜV, Telemedienrecht.</p> <p><b>3. Rechtliche Grundlagen für die Überwachung von Telekommunikationssystemen</b> Grundlagen zum Haftungsrecht (Zivil- und Deliktshaftung in Telekommunikationssystemen) und straf- sowie prozessrechtliche Grundlagen von Überwachungsmaßnahmen</p> <p><b>4. Datenschutzgesetze</b> Vermittlung grundsätzlicher Inhalte des Telemediengesetzes, Rundfunkstaatsvertrages, BGB-InfoV, insbesondere auch unter Sicht Informationsrechte und – pflichten sowie deren Rechtsdurchsetzung</p> <p><b>5. Rechtliche Regelungen zum Signaturgesetz und Verordnung zur digitalen Signatur</b> Voraussetzungen und Inhalte, insbesondere auch unter dem Aspekt der gem. § 126 a BGB geregelten elektronischen Form von Willenserklärungen und objektiver bzw. subjektiver Beweisführung</p> <p><b>6. Schutzrechte und Gewerblicher Rechtsschutz</b> Inhalte zum Urheberrecht / Digitales Urheberrecht; Patent / Gebrauchsmusterschutz; Marken / Domainrecht, Geschmacksmusterschutz; Wettbewerbsrechtliche Aspekte</p> <p><b>7. Recht der betrieblichen Sicherheit</b> Vermittlung von grundlegenden vertraglichen Voraussetzungen, dem Allgemeinen Gleichstellungsgesetz (AGG), Arbeitsschutzgesetze, Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit: Arbeitsstättenverordnung; Betriebssicherheitsverordnung; Bildschirmarbeitsplatzverordnung; Gefahrstoffverordnung .</p> <p><b>8. Waffenrecht</b> Regelungen des Waffengesetzes, insbesondere Bedürfnis, Zuverlässigkeit, Schusswaffenerwerb, Aufbewahrung, verbotene Waffen, Munitionsmeldung und rechtswidrige</p>

	bzw. erlaubte Anwendung von Waffen unter Zivil- und strafrechtlicher Sicht
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	1. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	6 ( Workload: 180 Stunden = 65 h Präsenz- und 115 h Eigenstudium)
Verantwortliche	Prof. Dr. Michaela Schröter
Lehrende	Prof. Schröter, Prof. Macke, Patentanwalt Herr Nitschke
Prüfungsform	Sonstige schriftliche Arbeit + Referat u./o. mündl. Prüfung
Zugangsvoraussetzungen	
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	<p><b>Gesetze:</b> BGB, ZPO, STGB, STPO, Insolvenzordnung, Arbeitsgesetze, Urheberrecht, Patentrecht, Telekommunikations- und Multimediarecht (aktuelle Ausgabe) Beck-Texte im dtv</p> <p><b>Grundlagenliteratur:</b> - Pannen (Hrsg): Europäische Insolvenzordnung, de Gruyter, 2007 - Eckardt/Klett: Wettbewerbsrecht, Gewerblicher Rechtsschutz und Urheberrecht, C. F. Müller, 2007 - Redeker: IT-Recht, Beck, 2007 - Knemeyer: Polizei- und Ordnungsrecht, Beck, 2007 - Däubler (Hrsg): Arbeitsrecht, Nomos, 2008 - Frenz: Handbuch Europa-Recht, Springer, 2007 - Prüthing/Wegen/Weinreich: BGB Kommentar, Heymann, 2007</p>
Lehr- und Lernmethoden	<p>Vorlesung mit gemischten Medien (Beamer und Folien). In Abstimmung mit den Teilnehmern wird jeweils vorbereitend auf das Thema der nächsten Veranstaltung die Angabe entsprechender Gesetze und aktueller Literatur und Beiträge erfolgen bzw. eine Auftragserteilung an die jeweiligen Teilnehmer die Veranstaltung und Diskussion eines Schwerpunktes vorzubereiten. Dies ermöglicht eine aktive und präzise Vorbereitung, sowie die Bewältigung der sehr umfangreichen Problematik in der Vorlesungszeit. Insbesondere in Vermittlung der Kenntnisse zum Gewerblichen Rechtsschutz erfolgt eine gemeinsame Diskussion mit einem Patentanwalt zur Rechtsanwendung. Aktuelle Rechtssprechung und juristische Beiträge sind entsprechend der Themen ständige Studien- und Diskussionsgrundlage.</p>
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Vertiefende, benotete sonstige schriftliche Arbeit zu einem Thema aus dem oben beschriebenen Themenkreis
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	



**4.2 Unternehmensführung, Personal- und Konfliktmanagement**

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Unternehmensführung, Personal- und Konfliktmanagement
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Die Studenten sollen aktuelle Methoden und Konzepte zur Unternehmensführung kennen lernen. Dabei soll insbesondere auf kritische Unternehmenssituationen und deren Analyse und Überwindung eingegangen werden.
Inhalt der Lehrveranstaltung	<ul style="list-style-type: none"> <li>• Funktionen der Unternehmensführung (Entwicklung von Unternehmensziele, -grundsätze, -kultur; Formulierung von Strategien; Personal- und Verhandlungsführung; internationale Aspekte im globalen Wettbewerb)</li> <li>• Ethische Aspekte der Unternehmensführung (Anti-Korruptionsstrategien, Code of Conduct etc.)</li> <li>• Risikomanagement</li> <li>• Krisenmanagement (Theorien zur Unternehmenskrisen, Methoden der Krisenerkennung, Krisenbewältigung, Rechtsnormen)</li> <li>• Konfliktmanagement (Konfliktdiagnose, Typologie von Konflikten, Eskalationen, Strategien zur Konfliktbehandlung)</li> </ul>
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	2. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	3 (Workload: 90 Stunden = 32 h Präsenz- und 58 h Eigenstudium)
Verantwortliche	Prof. Dr. Robert U. Franz
Lehrende	Prof. Dr. Robert U. Franz
Prüfungsform	Projektarbeit + Referat; u./o. mündl. Prüfung
Zugangsvoraussetzungen	
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	<p>K. Macharzina: Unternehmensführung  T. Hutzschenreuther: Krisenmanagement  F. Glasl: Konfliktmanagement</p> <p>Es werden Fallbeispiele während der Lehrveranstaltung konstruiert, die sich an aktuellen Nachrichten oder an Firmenideen anlehnen.</p> <p>Es werden Vorlesungsunterlagen in Form von Folien, Fallstudien und Übungsblättern über das Lehrelaufwerk als PDF-Dokumente zur Verfügung gestellt.</p>
Lehr- und Lernmethoden	Vorlesung mit vertiefender Projektarbeit und Rollenspielen

---

Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Projektarbeit mit abschließender mündlicher Prüfung
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	Die Vorlesung soll anhand von Fallbeispielen und/oder Planspielen sowie durch Vorträge von Gastreferenten anhand praxisrelevanter Beispiele unterstützt werden.

## 5 Sonstige Studienleistungen

### 5.1 Semesterarbeit 1 und 2

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Semesterarbeit 1 und Semesterarbeit 2
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Die Studierenden sollen ihre Fähigkeit zur selbstständigen wissenschaftlichen Auseinandersetzung mit einer Frage aus dem Bereich des Sicherheitsmanagements verbessern/ erweitern und hiermit Vorarbeiten zu einer qualitativ hochwertigen Master-Arbeit leisten. Die Semesterarbeiten eins und zwei können dabei inhaltlich aufeinander aufbauen, wobei Themen aus der Praxis die Grundlage der Arbeit bilden können.
Inhalt der Lehrveranstaltung	<ol style="list-style-type: none"> <li>1. Erhebungsmethoden (Statistik, Interview, primär/sekundär Quellen)</li> <li>2. Quellendiskussion vertiefen: recherchieren, lesen, bewerten</li> <li>3. Kreativtechniken und Selbstorganisation</li> <li>4. situationsbezogene Anforderungen an Schreibstile (Werbung, Pressemitteilung, wiss. Arbeit ...)</li> <li>5. Erstellen von wissenschaftlichen Arbeiten</li> <li>6. Erstellung eines Exposee's</li> <li>7. Methodischer Aufbau wiss. Arbeiten</li> <li>8. Sinn und Zweck einer wissenschaftlichen Arbeitsgruppen</li> <li>9. Phasen des wissenschaftlichen Arbeitens <ol style="list-style-type: none"> <li>1. Materialsammlung und Recherche</li> <li>2. Materialbewertung und -Auswahl</li> <li>3. Material- und Themenbearbeitung</li> </ol> </li> <li>10. Zitierweisen</li> </ol>
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	1. und 2. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	3 ( Workload: 90 Stunden = 30 h Präsenz- und 60 h Eigenstudium)
Verantwortliche	Prof. Dr. Friedrich-L. Holl; Dipl. Wi-inform Andreas Witt
Lehrende	Prof. Dr. Friedrich-L. Holl sowie alle anderen am SG beteiligten Lehrenden
Prüfungsform	Sonstige schriftliche Arbeit + Referat
Zugangsvoraussetzungen	

Empfohlene Literaturliste (Lehr- und Lernmaterialien, 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, 11. unveränd. Aufl. d. dt. Ausg. Theisen, Manuel R.: Wissenschaftliches Arbeiten - Technik Methodik, Form, 2000. Peterßen, Wilhelm H.: Wissenschaftliche(s) Arbeiten - Eine Einführung für Schule und Studium, 1999.
Lehr- und Lernmethoden	Übung in kleinen Gruppen
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Benotete Semesterarbeit und Verteidigung am Ende des Semesters
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gast sprecher etc.)	

## 6 Wahlpflicht und Projekte

### 6.1 *Projekt*

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Projekt
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	<p>Die Studierenden sollen anhand einer komplexen, möglicherweise im Wahlpflichtbereich begonnenen und hier weiterzuführenden Aufgabenstellung umfassende Kenntnisse im Umgang mit multikontextuellen Problemstellungen erlangen. Ziel ist die Herstellung von im Sicherheitskontext notwendigem ganzheitlichem Denken. Die Lehrinhalte in den Projekten sind neben den unten dargestellten methodischen Inhalten, deren Vermittlung ebenfalls zum Ziel der Lehrveranstaltung gehört, abhängig von der Themenwahl der Studierenden.</p> <p>Projektvorschlag 1: Internet-Kriminalität: In den vergangenen Jahren hat die Internet-Kriminalität in Deutschland rasant zugenommen. Die in diesem Zusammenhang auftretenden Probleme reichen von Dialern und Gewinnversprechen über Schäden durch Viren und Würmer bis hin zu verfassungsfeindlichen Inhaltsangeboten, Betrügereien bei Online-Auktionen und Datenschutzverletzungen. Im Rahmen des Projektes werden sich die Studierenden vorrangig selbstständig und auf wissenschaftlichem Niveau mit einer Aufgabenstellung aus dem großen Bereich der Internet-Kriminalität auseinandersetzen und ihre Ergebnisse und Schlussfolgerungen präsentieren.</p> <p>Projektvorschlag 2: Anwendungssysteme: In diesem Projekt haben die Studierenden die Möglichkeit, sich unter realitätsnahen Laborbedingungen intensiv mit der Auswahl, Konfiguration und Anpassung von Anwendungssoftware hinsichtlich sicherheitstechnischer Aspekte auseinanderzusetzen. Als zu untersuchende Software- Systeme kommen hierfür beispielsweise Datenbank-Server und Datenbank-Anwendungen und Software- Produkte für die Steuerung und Planung von Unternehmen in Frage. Die Studierenden beschäftigen sich im Rahmen des Projektes vorrangig selbstständig mit einer speziellen Problematik und dokumentieren und präsentieren zum Semesterende ihre Ergebnisse.</p> <p>Projektvorschlag 3: komplexes Security Scenario (Gepäckmanagement Flughafen, Sicherung eines größeren räumlichen Umfelds; Sicherung eines Lager mit hochwertigen Gütern usw.): Die Studierenden erheben den Stand der Technik bspw. über Besuche bei entsprechende Firmen und/oder Betreibern solcher Sicherheitslösungen, analysieren die Systeme auf Schwachstellen und entwickeln Soll-Konzepte,</p>

	<p>wie diese Szenarien zukünftig aussehen könnten. Hierbei geht es insbesondere darum, innovative Lösungsmöglichkeiten herauszuarbeiten und darauf aufbauend Vorschläge für Anträge auf Forschungs- und Entwicklungsvorhaben zu entwickeln. Hintergrund ist, dass darauf aufbauend Themen für forschungsorientierte Masterarbeiten entstehen sollen.</p>
Inhalt der Lehrveranstaltung	<p>Problemerkennung:</p> <ul style="list-style-type: none"> <li>- wissenschaftliche Erarbeitung des „State of the Art“</li> <li>- Einbindung in den vorhandenen praktischen Kontext</li> <li>- Rahmenbedingungen des Einsatzes</li> <li>- Nutzung unterschiedlicher Analysetechniken wie bspw. Interviewmethode, Fragebogen Delphimethode, Erarbeitung der Kontextes über Dokumente usw.</li> </ul> <p>Schwachstellenanalyse:</p> <ul style="list-style-type: none"> <li>- Vergleiche der bestehenden Anwendungen/ Voraussetzungen mit möglichen Entwicklungen</li> </ul> <p>Sollkonzeptentwicklung:</p> <ul style="list-style-type: none"> <li>- wissenschaftlich fundierte Entwicklung eines praxisorientierten Lösungsansatzes</li> <li>- Nutzung von Kreativmethoden</li> <li>- Kosten- Nutzen – Analysen</li> <li>- Entwicklung von Rahmenbedingungen des Einsatzes</li> </ul> <p>Prototypische Umsetzung</p> <ul style="list-style-type: none"> <li>- die prototypische Umsetzung erfolgt durch Entwicklung eines Software-Prototypen</li> <li>- Umsetzung im Unternehmen/ Organisation</li> </ul> <p>oder Entwicklung bspw. eines Antrags auf Forschungs- und Entwicklungsförderung</p> <p>Die gesamte Veranstaltung ist unter Gesichtspunkten des Projektmanagements zu organisieren</p>
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	2. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	3 ( Workload: 90 Stunden = 30 h Präsenz- und 60 h Eigenstudium)
Verantwortliche	Prof. Dr. Friedrich-L. Holl; Dipl. Wi-inform Andreas Witt
Lehrende	Prof. Dr. Friedrich-L. Holl sowie alle anderen am SG beteiligten Lehrenden
Prüfungsform	Projektarbeit + Referat
Zugangsvoraussetzungen	ggfs. notwendige Kenntnisse aus einem Wahlpflichtfach (abhängig vom Projektkontext)
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	Abhängig vom jeweiligen Kontext des durchgeführten Projektes
Lehr- und Lernmethoden	Projektarbeit in Gruppen bis maximal 7 Personen mit und in Unternehmen/ Organisationen, Dokumentation der

---

	Ergebnisse in wissenschaftlicher Arbeitsweise
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Ein Projektbericht am Ende des Semesters mit Verteidigung von beteiligten Unternehmen/ Organisationen
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	Hohe Unternehmens- und Praxisorientierung

## 6.2 Wahlpflichtfächer 1, 2 und 3

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	Wahlpflichtfach 1, Wahlpflichtfach 2, Wahlpflichtfach 3,
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	Die Studierenden sollen durch den Besuch der Wahlpflichtveranstaltung ihre Spezialisierungsziele möglichst individuell verfolgen können. Die Wahlpflichtfächer werden vorrangig im Zusammenhang mit praxisorientierten Fragestellungen der beteiligten Unternehmen/ Organisationen generiert.
Inhalt der Lehrveranstaltung	<p>Inhaltlich können die Projekte in den Bereichen Security Management, Gebäudesystemtechnik, Computer-Forensik, Internetkriminalität, Katastrophenmanagement, Personen- und Wachschutz, Sicherheits-Audits, Sicherheitsberatung usw. angesiedelt sein</p> <p>Beispielprojekt: Sicherheit bei Voice over IP (VOIP) Die inzwischen starke Verbreitung der VOIP-Technologie hat gezeigt, dass im Gegensatz zur traditionellen Telefonie grundsätzliche Sicherheitsprobleme auftretend. Im Rahmen der Ausarbeitung dieses Themas im Wahlpflichtfach wurde bspw. auf die Probleme Kompromittierung des Systems, Anonymität im Zusammenhang mit der Verwendung des Systems, Vertraulichkeit der Daten, Betrugsmöglichkeiten, Datenschutzkonformität usw. Eingegangen. Einen weiteren Teil bildet die praktische Erprobung sowie die darauf aufbauende Entwicklung von Checklisten und (möglichen) Sicherheitskonzepten.</p> <p>Als weiteres Wahlpflichtfach wird die Organisation eines Kongresses (Security –Forum) angeboten. Hier können die Studierenden sowohl ihren eigenen inhaltlichen Blick auf das von ihnen vertretene Verständnis von „Security Management“ umsetzen als auch Randgebiete des Security Managements kennenlernen und so die für den späteren Beruf erforderliche Sensibilität für die Gesamthematik erlangen. Zudem lernen sie über die Organisation einer derartig komplexen Veranstaltung, welche Voraussetzungen die Sicherung eines solchen Events verlangt (Ausfallvorsorge, Sicherung des Zugangs usw.). Über die inhaltliche Auseinandersetzung mit den Vortragenden ergeben sich zudem neue fachliche Erkenntnisse, die dann in den weiteren Veranstaltungen vertieft werden können.</p>
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Wahlpflicht
Semester/Trimester	1. oder 3. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	3 ( Workload: 90 Stunden = 30 h Präsenz- und 60 h Eigenstudium)
Verantwortliche	Prof. Dr. Friedrich-L. Holl; Dipl. Wi-inform Andreas Witt

Lehrende	anderen am SG beteiligten Lehrenden sowie speziell für ein besonderes WPF verpflichtete Lehrbeauftragte
Prüfungsform	Sonstige schriftliche Arbeit + Referat u./o. mündl. Prüfung
Zugangsvoraussetzungen	
Empfohlene Literaturliste (Lehr- und Lernmaterialien, Literatur)	Wird jeweils festgelegt
Lehr- und Lernmethoden	Übungen mit Vortragsanteil in kleinen und kleinsten (minimal 2 Teilnehmer) Gruppen
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Benotete Belegarbeit und Verteidigung am Ende des Semesters
Unterrichts-/Lehrsprache	Deutsch
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	Wahlpflichtfächer werden teilweise im direkten Umfeld der beteiligten Unternehmen/ Organisationen durchgeführt

## 7 Masterseminar / Masterarbeit mit Kolloquium

Bezeichnung der Lehrveranstaltung (Studien- bzw. Vertiefungsrichtung)	<b>Masterseminar / Masterarbeit mit Kolloquium</b>
Ziel der Lehrveranstaltung (erwartete Lernergebnisse und zu erwerbende Kompetenzen)	<p>Das Masterseminar dient zum Erwerb von Fähigkeiten zur Verknüpfung von Projektergebnissen und wissenschaftlichen Aufgabenstellungen, sowie zur Ableitung wissenschaftlicher Erkenntnisse aus Projektarbeiten und der methodischen Qualifizierung internationaler Forschungs- und Konferenzarbeiten. Die Master-Arbeit dient der zusammenhängenden Beschäftigung mit einem umfassenden Thema und der daraus resultierenden Lösung einer theoretischen oder praktischen Problemstellung.</p> <p>Die Master-Arbeit soll zeigen, dass der Kandidat in der Lage ist, innerhalb einer Frist von 4 Monaten eine Fragestellung auf dem Gebiet ‚Security Management‘ selbständig mit Hilfe wissenschaftlicher Methoden zu bearbeiten.</p> <p>Das Master-Kolloquium dient der Präsentation der Masterarbeit, einer wesentlichen Grundlage des angestrebten Abschlusses des Kandidaten. Im Rahmen dieser mündlichen Prüfung stellt der Kandidat seine Masterarbeit vor und stellt sich den Fragen des Plenums.</p>
Inhalt der Lehrveranstaltung	<p>Die Master-Arbeit ist eine Abschluss- Arbeit mit Kolloquium mit einem Aufwand von 21 CP. Begleitend findet ein Seminar statt, welches unbenotet bewertet wird und sich mit weiterführenden wissenschaftliche Arbeitstechniken, Standards des wissenschaftlichen Arbeitens mit Cases und dem Training wissenschaftlicher Kommentartechniken befasst. Die Bearbeitungszeit der Master-Arbeit beträgt 4 Monate. Die Master-Arbeit dient der zusammenhängenden Beschäftigung mit einem umfassenden Thema und der daraus resultierenden Lösung einer theoretischen oder praktischen Problemstellung.</p>
Art der Lehrveranstaltung (Pflicht, Wahl, etc.)	Pflicht
Semester/Trimester	3. Semester
Zahl der zugeteilten ECTS-Credits (basierend auf dem Arbeitspensum)	<p>Der Aufwand für das Masterseminar entspricht 3 CP ( Workload: 90 Stunden = 30 h Präsenz- und 60 h Eigenstudium)</p> <p>Die Masterarbeit umfasst mindestens 60 Seiten. Die Bearbeitungszeit beträgt 4 Monate. Der Aufwand incl. Kolloquium (Workload: ca. 90 Stunden) entspricht 21 CP.</p>

Verantwortliche	Prof. Dr. Friedrich Holl; Dipl. Wi.-Inform.(FH) Andreas Witt
Lehrende	Alle Lehrenden des SG Security-Management als Erstgutachter
Prüfungsform	Master-Arbeit und Mündliche Prüfung
Zugangsvoraussetzungen	Das Thema der Master-Arbeit kann nur erhalten, wer alle Prüfungsleistungen und Studienleistungen, die bis einschließlich des 2. Semesters zu erbringen sind. Das Kolloquium zur Master-Arbeit kann nur stattfinden, wenn keine Prüfungs- oder Studienleistungen offen sind.
Empfohlene Literaturliste (Lehr- und Lernmaterialien, 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, 11. unveränd. Aufl. d. dt. Ausg. Theisen, Manuel R.: Wissenschaftliches Arbeiten - Technik Methodik, Form, 2000. Peterßen, Wilhelm H.: Wissenschaftliche(s) Arbeite Eine Einführung für Schule und Studium, 1999. Gerorg G. Colomb, Joseph M. Williams, Wayne C. Booth: The Craft of Research, Third Edition, 2008 Sharon Sorenson: How to Write Research Papers v. 2, 1997 Motamedi, S.: Präsentation - Ziele, Konzepte, Durchführung, Heidelberg 1998.
Lehr- und Lernmethoden	Eigene wissenschaftliche Arbeit und Präsentation
Bewertungsmethoden (Lernkontrolle/ Leistungsüberprüfung auch Dauer der Prüfung)	Für die Bewertung der Master-Arbeit werden die Note der schriftlichen Arbeit mit 0,75 und die Note des Kolloquiums mit 0,25 gewichtet.
Unterrichts-/Lehrsprache	Die Master-Arbeit ist – nach Absprache mit dem Betreuer – entweder in Deutsch oder in Englisch zu verfassen. Mit Genehmigung des Prüfungsausschusses ist auch eine andere Sprache zulässig. Gleiches gilt für das Kolloquium.
Besonderes (z.B. Online-Anteil, Praxisbesuche, Gastsprecher etc.)	