Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modulhandbuch

Fakultät Informatik
Studiengang Business and Security Analytics

StuPO 17.2
ab Wintersemester 2020/21
Ersteller: Prof. Dr. German Nemirovski, Studiendekan
Verantwortlich: Prof. Dr. German Nemirovski, Studiendekan

Inhaltsverzeichnis

1 Vorwort

Der Masterstudiengang Systems Engineering ist ein praxisorientierter Master-Studiengang. Die Inhalte Werden auf wissenschaftlichem Niveau bei einer ausgeprägten Anwendungsorientierung vermittelt. Die Studierenden erlangen Qualifikationen, die sie befähigen als technische Fach- und Führungskräfte, weltweit aber auch für die regionale mittelständische Industrie tätig zu sein. Die Fähigkeiten, Fertigkeiten und Kenntnisse der Absolventen ermöglichen die folgenden Tätigkeitsfelder:

- Business Intelligence und Digitalisierung bei Beratungen sowie in Unternehmensabteilungen
- Analyst-Referent(in) direkt zugeordnet zum Direktorium oder Vorstand
- Risikomanagement bei Finanz-Unternehmen
- (IT-)Sicherheitsbeauftragte
- Security Information and Event Management

Folgende Qualifikationsziele werden in der Lehre gesetzt:

Konzeptionelle Fähigkeiten
Die Studierenden sind in der Lage, eigenständig Konzepte für Business Analytics-Werkzeuge und deren wirtschaftlichen Einsatz im Unternehmensumfeld zu entwickeln. Besondere Bedeutung hat in diesem Zusammenhang die Fähigkeit, theoretische Konzepte auf die konkreten Anwendungsfälle zu übertragen.
Vernetztes Denken
Die Studierenden können Zusammenhänge aus unterschiedlichen Anwendungsgebieten innerhalb des Fachgebiets und in deren Umfeld herleiten. Sie sind in der Lage, fachübergreifend zu analysieren und Konzepte zu entwickeln.
Führungskompetenz
Die Studierenden entwickeln sich in ihrer Führungsfähigkeit weiter. Sie sind in der Lage, Zielvereinbarungen zu treffen und deren Umsetzung zu steuern. Sie können ein Team motivieren und die Erfahrung von Personen unterschiedlicher Kompetenzen zielgerichtet zum Erfolg eines Teamprojekts einsetzen und nutzen.
Methodenkompetenz
Die Studierenden verfügen nicht nur über die Kenntnis von Methoden und Verfahren unterschiedlicher Fachgebiete der Informatik, sondern sind auch in der Lage, diese im jeweiligen Anwendungskontext anzuwenden.
Forschungskompetenz
Im Bereich Wissenschaft und Forschung sind die Studierenden in der Lage, wissenschaftliche Methoden einzusetzen und diese managementgerecht aufzubereiten.
Prozesskompetenz
Die Studierenden sind in der Lage, Konzepte und Strategien im Unternehmensumfeld erfolgreich umzusetzen. Sie haben das Rüstzeug, auch große Projekte von hoher Komplexität erfolgreich zu managen.
Analytische Kompetenz
Die Studierenden sind in der Lage, die für deren Problembereich relevanten Datenquellen zu identifizieren, die Daten formal zu beschreiben und diese für analytische Zwecke aufzubereiten. Sie sind darüber hinaus in der Lage, analytische Untersuchungen der Daten unter der Zielsetzung der Beantwortung komplexer Fragestellungen und des Generierens neuen, nicht trivialen Wissens selbstständig durchzuführen.

Sicherheitskompetenz
Die Studierenden sind in der Lage, im Rahmen einer eigenständigen Arbeit komplexe IT - Sicherheits und -Bedrohungs-relevanten Fragen und Problemstellungen zu formulieren. Sie sind in der Lage mit analytischen Mitteln aus Vorgangsdaten relevante Informationen zu Bedrohungen und Angriffen abzuleiten.

Ethische Kompetenz
Die Studierenden sind in der Lage ihr Vorgehen im rechtlich zulässigen, ethischen und moralischen Rahmen einzuordnen und kritisch zu hinterfragen. Insbesondere sind sie in der Lage Datenerhebungs- und Datenverarbeitungsprozesse bezüglich Konflikten mit Datenschutz- und Persönlichkeitsrechten zu prüfen.

2 Übersicht der Modulbeschreibungen

2.1 1. Semester

51100	Business Intelligence
51200	Data- and Webmining
51300	Large-Scale Data Analysis and Parallelization
51400	Semantic Web
51500	Strategic IT Management
51600	Open Source Intelligence
51700	Incident Response und Malware Defence

2.2 2. Semester

52100	Business Process Management and Data Compliance
52200	Advanced Statistic
52300	Distributed Enterprise Applications
52400	Financial Risks and Financial Management
52500	Innovation and Transfer Competence
52600	Advanced Network and Internet Security
52700	Security Analytics

2.3 3. Semester

60100	Master-Thesis
60200	Mündliche Masterprüfung

3 Qualifikationsziel-Modul-Matrix

Kompetenzen		Fachkompetenz						Personale Kompetenz				
		Wissen			Fertigkeiten			Sozialkompetenz		Selbständigkeit		
Ausprägung		Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungsfähigkeit	Team-/Führungsfähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit/ Verantwortung	Reflexivität	Lernkompetenz
51100	Business Intelligence	7	7	7				7			7	
52200	Advanced Statistics	7		7					7	7		
52300	Distributed Enterprise Applications	7		7						7		
52700	Security Analytics	7	7	7	7		7			7		7
51500	Strategic IT-Management		7	7	7		7		7	7		
52100	Business Process Management & Data Compliance	7		7			7		7	7		
51200	Data- and Webmining	7	7	7	7				7	7		
51300	Large-Scale Data Analysis & Parallelization	7	7	7			6			7		
51400	Semantic Web	7		6	7				7			7
52500	Innovations- und Transferkompetenz		7	7	7		7			7		
51600	Open Source Intelligence	6	7		7	7			7	7		7
51700	Incident Response and Malware Defence	7			7				7	7		
52600	Advanced Network and Internet Security	7		7	7					7		
52400	Finance Risk Management	7		7			7		7	7		7
60100	Master Thesis				7					7		
52400	Mü. Masterprüfung				7							7

Unterstützung der Qualifikationsziele in den Modulen (0=keine Unterstützung, 1=indirekte Unterstützung, 2=direkte Unterstützung)

Strategisches Denken
Die Studierenden verfügen über Verständnis zur Analyse der für die Geschäftsabläufe relevanten Informationen, verstehen daraus Wissensstrukturen zu formen und auf der Grundlage des resultierenden Wissens die Strategien für einen qualifizierten Entscheidungsfindungsprozess abzuleiten.

4 Studiengangs-Kompetenzmatrix

Kompetenzen		Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
Ausprägung		Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit/ Verantwortung	Reflexivität	Lernkompetenz
51100	Business Intelligence	7	7	7				7			7	
52200	Advanced Statistics	7		7					7	7		
52300	Distributed Enterprise Applications	7		7						7		
52700	Security Analytics	7	7	7	7		7			7		7
51500	Strategic IT-Management		7	7	7		7		7	7		
52100	Business Process Management & Data Compliance	7		7			7		7	7		
51200	Data- and Webmining	7	7	7	7				7	7		
51300	Large-Scale Data Analysis & Parallelization	7	7	7			6			7		
51400	Semantic Web	7		6	7				7			7
52500	Innovations- und Transferkompetenz		7	7	7		7			7		
51600	Open Source Intelligence	6	7		7	7			7	7		7
51700	Incident Response and Malware Defence	7			7				7	7		
52600	Advanced Network and Internet Security	7		7	7					7		
52400	Finance Risk Management	7		7			7		7	7		7
60100	Master Thesis				7					7		
52400	Mü. Masterprüfung				7							7

5 Modulbeschreibungen

5.1 1. Semester

5.1.1 51100 – Business Intelligence

Studiengang: Business and Security Analytics
StuPO-Version: 18.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

<table>
<tr><td colspan="7">Modul: Business Inteligence</td></tr>
<tr><td colspan="2">Kennnummer
51100</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Business Intelligence
Project Business Intelligence</td><td>Sprache
Deutsch oder Englisch, wenn von den Modulteil-nehmern gewünscht (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Projekt: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den elementaren Aufbau von Data Warehouse Systemen und sind mit den zentralen Konzepten der Informationsvisualisierung vertraut [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, die Konzepte des Data Warehousing in realen Anwendungsszenarien konzeptionell und operativ umzusetzen. Sie können Kennzahlen mittels geeigneter Methoden visualisieren. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden erarbeiten gemeinsam Lösungsansätze zu vorgegebenen Fragestellungen [Mitgestaltung, 7]
Selbstständigkeit</td></tr>
</table>

	Konzeption und Aufbau von Szenarien zur Erfassung, Aufbereitung und Analyse von Kennzahlen wird in Bezug auf die jeweiligen Anforderungen kritisch diskutiert. *[Reflexivität, 7]*
4	**Inhalte*:*** Abgrenzung dispositive vs. operative Datenbestände (OLTP / OLAP) Data Warehouse Architekturen ETL-Prozesse (Datenqualität, Datenbereinigung, Transformation, etc. Logische und semantische Datenmodelle für Data Warehouses (Star-/Snowflake-Schema,…) Implementierung von Data Warehouses (MOLAP, ROLAP,..) spezielle Aspekte im Zusammenhang mit Data Warehouses (slowly changing dimensions,…) Date Warehouse Projekte (agiles Vorgehen) Aufbau eines Data Warehousing Prozesses mittels SAP BW on HANA Visualisierung von Kennzahlen Konzeption und Aufbau von Dashoards Visual Analytics (Reduktion von Darstellungsdimensionen, Visualisierung von Objekten auf Grundlage von Unähnlichkeitsmaßen…)
	Empfohlene Literaturangaben: Bauer, A, Günzel, H (Hrsg): Data Warehouse Systeme – Architekur, Entwickung, Anwendung, dpunkt verlag, 2013 Müller, R.M., Lenz, H.-J.: Business Intelligence, Springer Vieweg, 2013 Kemper, H. G., Mehanna, W., & Unger, C. : Business Intelligence– Grundlagen und praktische Anwendungen, Vieweg, Wiesbaden, 2004, ISBN:3834807192 Klein, A., Gräf, J.: Reporting und Business Intelligence, Haufe-Lexware, 2014, ISBN: 364804771X Sharda, T. Aronson, King, A.:Business Intelligence: A Managerial Approach, Pearson Verlag, 2008, ISBN: 013610066X Kohlhammer, J., Proff, D.U., Wiener, A.: Visual Business Analytics: Effektiver Zugang zu Daten und Informationen. dpunkt.verlag GmbH, 2014, ISBN: 3864900441
5	**Teilnahmevoraussetzungen:**
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Schriftliche Modulprüfung; erfolgreiche Bearbeitung der Aufgaben im Praktikum
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: Prof. Dr. Bernd Stauß, N.N.

10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.2 51200 – Data and Web Mining

Studiengang: Business and Security Analytics
StuPO-Version: 18.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Data and Web Mining						
Kennnummer **52200**	**Workload** 180 h	**Modulart** P	**Studiensemester** 1		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung Data- and Web-Mining Praktikum Semantic Web		**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 120	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS Praktikum: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die grundlegenden Methoden des Data- und Web-Mining. Sie verstehen die Konzepte, kennen die Funktionsmechanismen der Methoden sowie die Rahmenbedingungen für deren Einsatz. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage die Methoden des Data- und Web-Mining in realen Anwendungssituationen sinnvoll einzusetzen. Sie sind in der Lage aus eine Menge von in Frage kommenden Methoden die geeigneten auszuwählen und diese einzusetzen. *[Instrumentelle Fertigkeiten, 7]* Die Ergebnisse aus der Anwendung der Methoden können eingeordnet und kritisch bewertet werden. *[Beurteilungsfähigkeit, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage die Ergebnisse ihrer Analysen einem Fachkundigen zu erläutern. *[Kommunikation, 7]* *Selbstständigkeit*					

	Die Studierenden sind in der Lage, eigenständig Datenanalysen zu konzipieren, auszuführen und die Ergebnisse verständlich darzustellen. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** Grundlagen das Data- und Web Mining Prozessuale Sicht auf das Data Mining (Crisp-DM) Data Preprocessing (Data Cleansing, Missing Values, Dimensionsreduzierung…) Clusteranalyse (hierarchisch, partitionierend) Klassifikation (Entscheidungsbäume, einfache Neuronale Netze, Support Vector Machines,… Assoziations Daten (A-Priori, FP-Growth) Sequenzanalyse Web Mining (Web Content Analyse)
	Empfohlene Literaturangaben: Han, J et al. – Data Mining – Concepts and Techniques, Elsevier – Morgan Kaufmann, 3rd edit., 2012 Thomas A. Runkler, Data Mining –Methoden und Algorithmen intelligenter Datenanalyse, Springer Vieweg, 2010 Ian H. Witten, Eibe Frank, Mark A. Hall, Data Mining: Practical Machine Learning Tools and Techniques, 3rd edit., Elsevier, 2011; Florin Gorunescu, Data Mining: Concepts, Models and Techniques, Springer, 2011, Markus Hofmann, Ralf Klinkenberg, Rapidminer: Data Mining Use Cases and Business Analytics Applications, Productivity Pr Inc, 2013, Bing Liu, Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data (Data-Centric Systems and Applications), Springer; 2. Auflage, 2011, Beierle, C., Kern-Isberner, G. – Methoden wissensbasierter Systeme – Grundlagen, Algorithmen, Anwendungen, Vieweg+Teubner, 5. Aufl. 2014
5	**Teilnahmevoraussetzungen:** Es existieren keine Teilnahmevoraussetzungen.
6	**Prüfungsformen*:*** Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Die erfolgreiche praktische Arbeit im Praktikum wird durch Semesteraufgaben, die eigenständig zu bearbeiten sind, nachgewiesen.
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: Prof. Dr. Bernd Stauß, N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.3 51300 – Large Scale Data Analysis and Parallelization

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

<table>
<tr><td colspan="7">Modul: Large-Scale Data Analysis and Parallelization</td></tr>
<tr><td colspan="2">Kennnummer
51300</td><td>Workload
180 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Large-Scale Data Analysis and Parallelization
Praktikum Large-Scale Data Analysis and Parallelization</td><td>Sprache
Deutsch oder Englisch, wenn von den Modulteil-nehmern gewünscht (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
- kennen Systeme und Techniken für die parallele Datenverarbeitung
- kennen die Aufgabenstellungen aus dem Themengebiet von Big Data [Wissen, 7]
Kompetenz Fertigkeiten
Lernergebnisse (Kompetenzen) bei:
Die Studierenden
- sind in der Lage die Problem- und Aufgabenstellungen mit Bezug auf das Themengebiet Big Data zu erkennen, diese, basierend auf eigenem Wissen und durch die gezielte Recherche zu beschreiben, Lösungsansätze zu entwickeln und diese allein oder im Team umzusetzen.
- sind in der Lage, eine anwendungsbezogeneEvaluation von Daten, –Zugriffs- und –Verwaltungstechniken sowie von den diese Techniken implementierenden Systemen</td></tr>
</table>

	auszuführen, und darauf basierend eine zielgerechte Auswahl zu treffen. - sind in der Lage wissenschaftliche Beiträge im Themenbereich Big Data eigenständig zu lesen und qualitative Vergleiche der gelesenen Beiträge systematisch zu präsentieren. *[Instrumentelle Fertigkeiten, 7]*
	Sozialkompetenz Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen Big Data Prozess mit konkreter Aufgabenstellung entwickeln *[Team-/Führungsfähigkeit, 7]*
	Selbstständigkeit Die Studierenden sind in der Lage komplexe Aufgaben verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen. *[Eigenständigkeit/Verantwortung, 7]*

4	**Inhalte*:***
	Vorlesung:
	- Überblick zu No-SQL-Datenbanken
	- Überblick zu Graphendatenbanken
	- Architekturen für verteiltes und paralleles Datenmanagement und Datenverteilung
	- Verteilte Anfragebearbeitung
	- Clustering, Map Reduce, YARN, Tez
	- Verteilte Datenbanken
	  - Vertikale/horizontale Fragmentierung
	  - Fragmentierungstransparenz
	  - Transaktionskontrolle
	- Frameworks für Skalierung und Parallelisierung der Datenzugriffe am Beispiel von Apache Hadoop, Spark und verteilten RDBMS
	
	Praktikum:
	Arbeiten mit Apache Hadoop, Spark Clustern, IBM Cloud, Azure, IBM Data Warehouse
	Arbeiten mit MongoDB, Apache Cassandra, Neo4J
	Arbeiten mit Injectiontools wie Apache Nifi, Talend, IBM NodeRed

	Empfohlene Literaturangaben:
5	**Teilnahmevoraussetzungen:**
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.

9	***Modulverantwortliche(r):*** Prof. Dr. Thomas Eppler Dozenten: Prof. Dr. Thomas Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.4 51400 – Semantic Web

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Modul: Semantic Web					
Kennnummer 51400	**Workload** 180	**Modulart** WP	**Studiensemester** 1	**Dauer** 1	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** a. 51405 Semantic Web b. 51420 Proj. Semantic Web	**Sprache** a.,b., deutsch oder englisch	**Kontakt-zeit** a. 30 b. 30	**Selbst-studium** 120	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** a. Vorlesung, b. Projektarbeit				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Vertieftes verstehen Formaler Logiken und Reasoning-Aufgaben *[Wissen, 7]* Vertieftes Verstehen von Semantic Web -Technologien als Instrument für interoperable Wissensbeschreibung *[Wissen, 7]* *Kompetenz Fertigkeiten* Können Ontologien mit Hilfe von Tools wie Editoren und Reasoner entwickeln und Anwenden *[Instrumentelle Fertigkeiten, 6]* Können Wissensstrukturen von Komplexen Wissensdomains analysieren und formal beschreiben *[Systemische Fertigkeiten, 7]* *Sozialkompetenz* Sind in der Lage komplexe Formalismen zu kommunizieren und Diskussion auf Grundlage der Formalismen und mit Anwendung des formallogischen Vokabular zu führen *[Kommunikation, 7]* *Selbstständigkeit* Sind in der Lage komplexe Fragestellungen selbständig zu Bearbeiten und eigenen Fortschritt adäquat zu bemessen *[Lernkompetenz, 7]*				
4	Inhalte:				

	Die Grundlagen: - Definition und Begriffsklärung - Security Analytics Use Cases - Data Sourcess und Methoden der Datensammlung - Real time Data Harvesting - Anwendung der Security Analytics Ergebnissen und ihr Impact - Basic Security Analytics Costs - Advanced persistent threats - Security Analytics und Digitale Forensics Security Analytics Tools and Services, u.a.: - Blue Coat Security Analytics Platform, - Lancope Stealth Watch System - JuniperNetworks JSA Series Secure Analytics - EMC RSASecurity Analytics NetWitness - FireEye Threat Analytics Platform - Arbor Networks Security Analytics - Click Security Click Commander - Hexis Cyber Solutions' NeatBeat MON - Sumo Logics' cloud service. - Security Onion - Splunk - Elastic Stack
	Empfohlene Literaturangaben: Lehto, Martti, and Pekka Neittaanmäki, eds. Cyber security: Analytics, technology and automation. Vol. 78. Springer, 2015. Talabis, Mark, et al. Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. Syngress, 2014. THOMAS, TONY P. VIJAYARAGHAVAN, Athira P. Vijayaraghavan, and Sabu Emmanuel. MACHINE LEARNING APPROACHES IN CYBER SECURITY ANALYTICS. SPRINGER VERLAG, SINGAPOR, 2020.
5	**Teilnahmevoraussetzungen:** Kenntnisse in IT Security (DQR 6), Praktische Fertigkeiten in Netzwerken und Programmierung (DQR 6)
6	**Prüfungsformen***:* Klausur 90 Min. (Modulprüfung)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Business und Security Analysis MSc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski

10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.5 51500 – Strategic IT Management

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Modul: Strategic IT Management					
Kennnummer 51500	**Workload** 180 h	**Modulart** P	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung Strategic IT-Management Fallstudie Strategic IT-Management	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 120	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS Fallstudie: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden • kennen Zielstellung, Zielgruppen und den Aufbau von IT-Strategien • kennen Instrumente zur Planung, Steuerung und Kontrolle von IT-Bereichen • kennen die strategischen Herausforderungen der IT-Sicherheit im digitalen Zeitalter • kennen die strategische Bedeutung von IT Governance, Risk and Compliance Management (IT-GRC) für Unternehmen, IT-Organisation und CIO • kennen innovative Geschäftsmodelle der digitalen Plattformökonomie aus Sicht der IT *[Wissen, 7]*				
	Kompetenz Fertigkeiten Die Studierenden • können den Einsatz der Informationstechnologie im Kontext der strategischen Ausrichtung des Unternehmens bewerten und einordnen • können die Herausforderungen, Aufgaben und methodisches Vorgehen des IT-Management beschreiben • können die Auswirkungen von Digitalisierung und speziell der digitalen Plattformökonomie auf das IT-Management skizzieren • beherrschen die differenzierte Einordnung von IT-Sicherheit und IT-Governance,				

	Risk and Compliance Management (IT-GRC) in den Kontext des IT-Managements *[Instrumentelle Fertigkeiten, 7]* *Die Studierenden* • *können in umfangreichen, realitätsnahen Fallstudien die Unternehmenssituation analysieren, strategische Aspekte vor dem Hintergrund von Branche sowie Unternehmensumwelt bewerten, die Herausforderungen für IT-Organisationen und das IT-Management systematisieren* • *können weiterhin – durch zielgerichtete Abstraktionstechniken – Grundzüge von IT-Strategien und Maßnahmenkataloge für das IT-Management entwickeln* *[Systemische Fertigkeiten, 7]*
	Sozialkompetenz Die Studierenden sind in der Lage, die komplexen Fallstudien zum IT-Management – im Kontext aktueller Trends und Entwicklungen in IT und Digitalisierung – in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren [Team-/Führungsfähigkeit, 7] Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken auf Management-Niveau *[Kommunikation, 7]*
	Selbstständigkeit Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • IT-Strategieentwicklung • Rolle und Aufgaben der IT im Unternehmen • Rolle, Aufgaben und Pflichten des Chief Information Officer (CIO) im Unternehmen • Aufgaben, Rollen und Gremien im IT-Management • Aufbau von IT-Organisationen und internationale Koordination • Business-IT-Alignment mit internen und externen Kunden • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC) • IT-Service- und Prozessmanagement • IT-Ressourcenmanagement • Management des IT-Applikationsportfolios • IT-Partnermanagement: Relationship Management und Sourcing-Strategien • Sourcing Strategien: Business Process Outsourcing, Application Outsourcing, IT-Infrastruktur Outsourcing und Cloud Computing • IT-Projekt- und Projektportfoliomanagement • IT-Planung und IT-Controlling • IT-Management Cockpits • Umgang mit Schatten-IT • Digitalisierung, Digitale Transformation und Digitale Plattformökonomie • Industrie 4.0 im Kontext von Industrieunternehmen • IT-Unterstützung innovativer Geschäftsmodelle in der Plattformökonomie

	Empfohlene Literaturangaben: Porter, M. E.: Wettbewerbsstrategie: Methoden zur Analyse von Branchen und Konkurrenten, 12. Auflage, campus, 2013 Porter, M. E.: Wettbewerbsvorteile: Spitzenleistungen erreichen und behaupten, 8. Auflage, campus, 2014 Malik, F.: Strategie des Managements komplexer Systeme: Ein Beitrag zur Management-Kybernetik evolutionärer Systeme, 11. Auflage, 2015 Camenzind, A./Fueglistaller, U.: Strategisches Denken in KMU und die Lehren von Clausewitz, Verlag Neue Zürcher Zeitung, 2014 Simon, H./Von der Gathen, A.: Das große Handbuch der Strategieinstrumente: Werkzeuge für eine erfolgreiche Unternehmensführung, 2. Auflage, Campus, 2010 Hofmann, J./Schmidt, W.: Masterkurs IT-Management - Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker. 2. Auflage, Vieweg und Teubner, 2010 Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 7. Auflage, Hanser Verlag, 2020 Oswald G./Krcmar, H.: Digitale Transformation: Fallbeispiele und Branchenanalysen (Informationsmanagement und digitale Transformation), Springer Gabler, 2018 Krcmar, H.: Informationsmanagement, 6. Auflage, Springer, 2015 Resch, O.: Einführung in das IT-Management - Grundlagen, Umsetzung, Best Practice, 4. Auflage, Erich Schmidt Verlag, 2016 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 Zimmermann, S.: Der Umgang mit Schatten-IT in Unternehmen: Eine Methode zum Management intransparenter Informationstechnologie Hanschke, I.: Strategisches Management der IT-Landschaft: Ein praktischer Leitfacen für das Enterprise Architecture Management, 3. Auflage, Hanser Verlag, 2013 Kersten, H./Klett, G./Reuter, J./Schröder, K.-W.: IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, 4. Auflage, Springer Vieweg, 2019 Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung", Springer Vieweg, 2017 Mangiapane, M./Büchler, R.: Modernes IT-Management: Methodische Kombination von IT- Strategie und IT-Reifegrademodell, Springer Vieweg, 2015 Osterwald, A./Pigneur, Y.: Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer, campus, 2011 Osterwald, A./Pigneur, Y./Bernarda, G./Smith, A.: Value Proposition Design: Entwickeln Sie Produkte und Services, die Ihre Kunden wirklich wollen, campus, 2015 Gärtner, C./Heinrich. C. (Hrsg.): Fallstudien zur Digitalen Transformation: Case Studies für die Lehre und praktische Anwendung, Springer Gabler, 2017 Von Engelhardt, S./Petzold, S. (Hrsg.): Das Geschäftsmodell-Toolbox für digitale Ökosysteme, Campus, 2019 Srnicek, N.: Plattform-Kapitalismus, Hamburger Edition, 2018 Jaekel: Die Macht der digitalen Plattformen: Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz, Springer Vieweg, 2017 Parker, G. G./Van Alstyne, M.W./Choudary, S. P.: Die Plattform-Revolution im E-Commerce: Von Airbnb, Uber, PayPal und Co. lernen: Wie neue Plattform-Geschäftsmodelle die Wirtschaft verändern, mitp, 2017 Clement, R./Schreiber, D./Bossauer, P./Pakusch, C.: Internet-Ökonomie: Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, 4. Auflage, Springer Gabler, 2020

5	**Teilnahmevoraussetzungen:** Kenntnisse auf den folgenden Lehrgebieten sind hilfreich: • IT-Management, IT-Consulting und E-Business • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC)
6	**Prüfungsformen***:* Seminararbeit, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreich bearbeitete Seminararbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.6 51600 – Open Source Intelligence

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Modul: Open Source Intelligence						
Kennnummer 51600	**Workload** 180 h	**Modulart** WPM	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS	
1	**Lehrveranstaltung(en)** Vorlesung Open Source Intelligence Praktikum Open Source Intelligence	**Sprache** Deutsch oder Englisch (Literaturstudium in Deutsch und Englisch erforderlich)	**Kontakt-zeit** 60 SWS / 4 h	**Selbst-studium** 120	**Credits (ECTS)** 6	
2	**Lehrform(en) / SWS:** Vorlesung, Übungen, Seminar: 3 SWS Praktikum: 1 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen*					

	Die Studierenden verfügen über ein breites Wissen über die technischen, gesellschaftlichen und rechtlichen Rahmenbedingungen für einen OSINT Einsatz, *[Wissen, 6]* Die Studierenden verfügen über ein tiefes Wissen im Bereich von OSINT Terminologien, Methoden und Techniken, *[Wissen, 7]*
	Kompetenz Fertigkeiten Können einen OSINT Einsatz konzeptionell strukturieren und geeignete Methoden und Werkzeuge auswählen *[Instrumentelle Fertigkeiten, 7]* Können die Leistungsfähigkeit vorhandener OSINT Werkzeuge beurteilen und selbstständig neue OSINT Verfahren und Werkzeuge entwickeln *[Systemische Fertigkeiten, 7]* Können per OSINT ermittelte Daten hinsichtlich ihrer technischen und juristischen Verwertbarkeit beurteilen und ihren Informations- und Intelligence Gehalt einschätzen *[Beurteilungsfähigkeit, 7]*
	Sozialkompetenz Studierende können sich auf tiefer Expertenebene mit der Fachcommunity unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln *[Kommunikation, 7]*
	Selbstständigkeit Studierende können neue OSINT Anwendungen eigenständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren *[Eigenständigkeit/Verantwortung, 7]* Aktuelle Aufgabenstellungen und Probleme aus dem OSINT Bereich können eigenständig anhand der aktuellen Forschung im Print- und Preprintbereich erschlossen werden *[Lernkompetenz, 7]*
4	**Inhalte*:*** Vorlesung, Seminar, Praktikum • Auffrischung relevanter Grundlagen der IT Sicherheit, Digitalen Forensik und Internettechnologien • Anonymisierung und De-Anonymisierung im Surface-, Deep- und Darknet • Ermittlungstaktisches- / nachrichtendienstliches Vorgehen • OSINT Grundlagen, Terminologien, Taxonomien • OSINT Methoden, Tools, Techniken • Legaler, moralischer und ethischer Rahmen • Analyse und Bewertung von OSINT Erkenntnissen • Praktische Anwendungen • Wissenschaftliche Recherche, Arbeit und Forschung im OSINT Bereich • Relevante wissenschaftliche Konferenzen, Journals und Plattformen
	Empfohlene Literaturangaben: Akhgar, B., Bayerl, P.S., Sampson, F.S.: OpenSource Intelligence Investigation – From Strategy to Implementation, Springer, 2017 Bazzell, M.: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 5. Auflage, CreateSpace Independent Publishing Platform, 2016 U.S.Army: NATO OpenSource Intelligencehandbook, online, http://www.au.af.mil/au/awc/awcgate/nato/osint_hdbk.pdf

	Attrill, A.: Cyberpsychology, 2015, Oxford University Press Gollmann, D.: Computer Security, 3. Auflage, Wiley, 2012 Tavani, H.T.: Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, 4. Auflage, Wiley, 2013 Spinello, R.: Cyberethics: Morality and Law in Cyberspace 6th Edition, Jones & Bartlett Learning, 2016 A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology, 5th Edition, Pearson, 2017 Biskup, J.: Security in Computing Systems, Springer, 2010 Ausgewählte Literatur bekannter Top-Tier Konferenzen im OSINT Bereich Weitere Literatur wird in der Vorlesung vorgestellt.
5	**Teilnahmevoraussetzungen:** Grundlagen Betriebssysteme und Netzwerke, Grundlagen IT Sicherheit und Digitaler Forensik, Programmierung in einer Skriptsprache
6	**Prüfungsformen***:* Referat 20 min. inkl. wissenschaftlicher Ausarbeitungen und Poster, Diskussion, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics
9	***Modulverantwortliche(r):*** Prof. Morgenstern Dozenten: Prof. Dr. Fein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.7 51700 – Incident Response und Malware Defence

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Modul: Incident Response und Malware Defence						
Kennnummer 51700	**Workload** 180 h	**Modulart** P	**Studiensemester** 1		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung Incident Response und Malware Defense Praktikum Incident Response und Malware Defense		**Sprache** Deutsch	**Kontakt-zeit** 60 SWS / 4 h	**Selbst-studium** 120	**Credits (ECTS)** 6

2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS Praktikum: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können Methoden entwickeln und anwenden um IT-Angriffe zu erkennen, zu analysieren, einzudämmen und zu beseitigen *[Systemische Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen *[Eigenständigkeit/Verantwortung, 7]*				
4	**Inhalte*:*** 1. Der Incident Response Prozess: Preparation, Detection, Analysis, Containment, Recovery, Post Incident Activity Veranschaulichung und Vertiefung der Phasen an Beispielen 2. Klassifikation und Taxonomie von Incidents 3. Systemsicherung: Sicherung systemwichtiger Daten 4. Spurensicherung: Netzbasierte Spuren (Netzwerkmitschnitte und Netzwerk-Komponenten), Host-basierte Spuren (persistente und nicht persistente Spuren, Arbeitsspeicher) 5. Spurenanalyse: Netzbasierte Spuren (Netzwerkmitschnitte, Log-Dateien), Host-basierte Spuren (Arbeitsspeicher, Log-Dateien, Dateisysteme) 6. Detektion: Signatur-basierte und Regel-basierte Methoden 7. Methoden zur Einschränkung der Schadwirkung: Sandbox, Zugriffsschutz, Rechteüberwachung, Firewall, Proxy, Netzwerksegmentierung 8. Wiederherstellung: Backup und Systemsicherung anwenden 9. Statische Malware-Analyse: Aufbau der Malware, verwendete Bibliotheken, maliziöse Funktionen und Strukturen 10. Dynamische Malware-Analyse: Wirkungsweise der Malware, Schadwirkung lokalisieren 11. Reporting zur Malware-Analyse: Wirkungsweise, Schadenspotential, potentielle Quellen 12. Reporting zum Incident Response-Prozess 13. Post Incident Aktivitäten: Maßnahmen zur Verbesserung der Sicherheit treffen; Training von Incidents Beispiele für Projekte				

	• Aufsetzen einer Signaturbasierten Detektion in einem System. Angriff auf das System. Incident behandeln • Aufsetzen eines Systems mit Schwachstellen (z. B. offene USB-Anschlüsse oder Mail-Clients ohne Makrovirenschutz); Eintragen einer Malware; Incident Response Prozess ausführen • Entwicklung einer Malware, die vermutete Systemschwächen ausnutzt (z. B. Keylogger, DLL-Injektor); Erproben der Malware an einem System mit Malware-Schutz; Incident Respons anwenden
	Empfohlene Literaturangaben: Alan J White (Autor), Ben Clark: Blue Team Field Manual. Create Space Independent Publishing Platform (2017) Gerard Johansen: Digital Forensics and Incident Response.Packt (2012 Johansen, Gerard. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents (Kindle-Positionen14-15). Packt Publishing. Kindle-Version. Cameron H. Malin, Eoghan Casey, James M. Aquilina: Malware Forensics Guide for Windows Systems, Digital Forensics Field Guides. Elsevier (2012) Weitere Literatur, insbesondere aktuelle wissenschaftliche Artikel, werden in der Vorlesung bekannt gegeben.
5	Teilnahmevoraussetzungen: Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Praktische Arbeit mit Präsentation 20 min. und Handout, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2 2. Semester

5.2.1 52100 – Business Process Management and Data Compliance

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_Business and Security Analytics_FINAL-1.docx		

Studiengang: Business and Secvurity Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

<table>
<tr><td colspan="7">Modul: Business Process Management and Data Compliance</td></tr>
<tr><td colspan="2">Kennnummer
52100</td><td>Workload
180 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Business Process Management and Data Compliance
Fallstudie Business Process Management and Data Compliance</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Fallstudie: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen

Die Studierenden
• kennen Merkmale, Aufbau und Prinzipien von Prozessen und Geschäftsprozesse im Kontext der betrieblichen Ablauforganisationen
• kennen betriebliche Wertschöpfungsstrukturen und Anforderungen an das unternehmensweite Prozessmanagement
• kennen die gängigen Modellierungsmethoden und können diese auf Meta-Modellebene systematisieren
• kennen Kennzahlen und Kennzahlensysteme für das Monitoring von Geschäftsprozessen
• kennen den Datenbegriff und Methodiken zum Master Data Management
• kennen die Herausforderungen zum Datenschutz im Kontext der betrieblichen Erfassung, Verarbeitung und Speicherung personenbezogener Daten
• kennen Zielstellung, methodisches Vorgehen und Kontrollmechanismen zu Data Compliance, auch im digitalen Kontext [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden
• können betriebliche Ablaufstrukturen in gängigen Modellierungsnotationen modellieren und beherrschen den Einsatz von Abstraktionstechniken
• können betriebliche Prozesse auf Automationspotenzial und Resilienzfähigkeit hin analysieren und optimieren
• können Prozesse auf Basis von Kennzahlen und Kennzahlensystemen systematisieren und vergleichen sowie Monitoring- und Reporting-Strukturen aufbauen
• können den betrieblichen Datenschutz und Data Compliance-Strukturen beschreiben und systematisieren
[Instrumentelle Fertigkeiten, 7]</td></tr>
</table>

	Sozialkompetenz Die Studierenden sind in der Lage, die komplexen Fallstudien zu Business Process Management and Data Compliance – im Kontext aktueller Trends und Entwicklungen in IT und Digitalisierung – in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren [Team-/Führungsfähigkeit, 7] Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken auf Management-Niveau *[Kommunikation, 7]*
	Selbstständigkeit Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Prozesse und Geschäftsprozesse • Betriebliche Kernkompetenzen und unternehmensweite Kernprozesse • Betriebliche Wertschöpfung, Wertschöpfungsstufen und Wertschöpfungsketten • Prozessmanagement und Prozessportfolio • Operatives versus strategisches Prozessmanagement • Enterprise Architecture Management und Business Architecture Management • Aufbau und Vergleich von Modellierungsmethoden für den betrieblichen Einsatz • Meta-Modelle und Meta-Meta-Modelle • Referenzmodelle und Prozesslandkarten • Kennzahlen und Kennzahlensysteme für das Monitoring von Geschäftsprozessen • Daten und Master Data Management • Datenschutz im Kontext der betrieblichen Unternehmung • Erfassung, Verarbeitung und Speicherung von Daten im Kontext gesetzlicher Vorgaben (Bundesdatenschutzgesetz und Datenschutz-Grundverordnung) • Zielstellung, methodisches Vorgehen und Kontrollmechanismen zu Data Compliance • Data Compliance im Kontext von Digitalisierung und digitaler Plattformökonomie
	Empfohlene Literaturangaben: Hofmann, J./Schmidt, W.: Masterkurs IT-Management - Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker. 2. Auflage, Vieweg und Teubner, 2010 Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 7. Auflage, Hanser Verlag, 2020 Hanschke, I.: Strategisches Management der IT-Landschaft: Ein praktischer Leitfacen für das Enterprise Architecture Management, 3. Auflage, Hanser Verlag, 2013 Kersten, H./Klett, G./Reuter, J./Schröder, K.-W.: IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, 4. Auflage, Springer Vieweg, 2019 Schmelzer, Herrmann J./Sesselmann, Wolfgang: Geschäftsprozessmanagement in der Praxis: Kunden zufrieden stellen, Produktivität steigern und Wert erhöhen, Hanser, 2013 Keuper, Frank/Neumann, Fritz: Corporate Governance, Risk Management und Compliance: Innovative Konzepte und Strategien,Gabler, 2010

	Nestler, D./Modi, J. (Hrsg.: Institut der Wirtschaftsprüfer in Deutschland e.V.): Leitfaden IT-Compliance: Anforderungen, Chancen und Umsetzungsmöglichkeiten, IDW, 2020. Klotz, M.: IT-Compliance: Ein Überblick, 1. Auflage, dpunkt, 2009 Rath, M.; Sponholz, R.: IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen, o. A., Erich Schmidt, 2009 Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung", Springer Vieweg, 2017 Sowa, A./Duscha, P./Schreiber, S.: IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die IT-Prüfung, Springer Vieweg, 2019 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 Gärtner, C./Heinrich. C. (Hrsg.): Fallstudien zur Digitalen Transformation: Case Studies für die Lehre und praktische Anwendung, Springer Gabler, 2017 Von Engelhardt, S./Petzold, S. (Hrsg.): Das Geschäftsmodell-Toolbox für digitale Ökosysteme, Campus, 2019 Srnicek, N.: Plattform-Kapitalismus, Hamburger Edition, 2018 Jaekel: Die Macht der digitalen Plattformen: Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz, Springer Vieweg, 2017 Parker, G. G./Van Alstyne, M.W./Choudary, S. P.: Die Plattform-Revolution im E-Commerce: Von Airbnb, Uber, PayPal und Co. lernen: Wie neue Plattform-Geschäftsmodelle die Wirtschaft verändern, mitp, 2017 Clement, R./Schreiber, D./Bossauer, P./Pakusch, C.: Internet-Ökonomie: Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, 4. Auflage, Springer Gabler, 2020
5	**Teilnahmevoraussetzungen:** Kenntnisse auf den folgenden Lehrgebieten sind hilfreich: • IT-Management, IT-Consulting und E-Business • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC)
6	**Prüfungsformen***:* Mündliche Prüfung (20 min.), benotet Referat, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreich bearbeitete Seminararbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozenten: Prof. Dr. Nils Herda, Prof. Dr. Bernd Stauß
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.2 52200 – Advanced Statistic

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

<table>
<tr><td colspan="8">Modul: Advanced Statistics</td></tr>
<tr><td colspan="2">Kennnummer
52200</td><td>Workload
180 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung & Seminar Advanced Statistics
Übungen Advanced Statistics</td><td>Sprache
Deutsch und Englisch (deutsches und englisches Litaratur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung & Seminar: 2 SWS
Übungen: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierende kennen die grundlegenden Begriffe der Wahrscheinlichkeitstheorie und können diese anwenden [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können den Stoff praktisch in der Programmiersprache R für Analysen umsetzen [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden können statistische Sachverhalte anderen vermitteln. [Kommunikation, 6]
Selbstständigkeit
Die Studierenden können selbstständig Analysen mittels der Programmiersprache R durchführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
R-Grundlagen.

Stochastische Grundlagen (Wahrscheinlichkeit, Bedingte Wahrscheinlichkeit, Satz von Bayes)
Zufallsvariablen, Erwartungswert, Varianz, Stichproben, Lage- und Streumaße

Bootstrapping, Konfidenzintervalle, Verteilungen (Binomialverteilung, Poisson-Verteilung, Geometrische Verteilung, Exponentialverteilung, Normalverteilung,</td></tr>
</table>

	Betaverteilung) Signifikanz- und Hypothesentests (A/B-Tests, Permutationstests, ANOVA), Korrelationen, Maximum-Likelihood, Lineare Regression.
	Empfohlene Literaturangaben: Introduction to Statistical Thought☐ISBN: 978-1616100483 http://people.math.umass.edu/~lavine/Book/book.html Introduction to Probability and Statistics UsingR ISBN: 978-0-557-24979-4 http://cran.r-project.org/web/packages/IPSUR/vignettes/IPSUR.pdfAn Introduction to Statistical Learning: with Applications in R Gareth James, Daniela Witten, Trevor Hastie, Robert TibshiraniSpringer Texts in Statistics, 11. Juli 2016, ISBN-10: 1461471370 Die "'offizielle"' R-Einführung☐ISBN: 978-0954612085 cran.r-project.org/doc/manuals/R-intro.pdf R-Kurs der Uni Augsburg: stats.math.uni-augsburg.de/~theus/r-kurs.pdf
5	**Teilnahmevoraussetzungen:** Grundlegende Programmierkenntnisse müssen da sein.
6	**Prüfungsformen***:* Klausur 90 min., benotet Referat, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Tobias Häberlein Dozenten: Prof. Dr. Tobias Häberlein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.3 52300 – Distributed Enterprise Applications

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Modul: Distributed Enterprise Applications					
Kennnummer 51300	**Workload** 180 h	**Modulart** WPM	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)**	**Sprache**	**Kontakt-zeit**	**Selbst-studium**	**Credits (ECTS)**

	Vorlesung Distributed Enterprise Applications Projekt Distributed Enterprise Applications	Deutsch, bei Bedarf Englisch (muss vor Semester-beginn geäußert werden)	4 SWS / 60 h	120	6
2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS Übungen: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die Bedeutung und Notwendigkeit der Betrachtung und Entwicklung von Software-Architekturen für komplexe und vor allem verteilter Software-Produkte, Architekturmuster zur Implementierung verteilter Anwendungen, Techniken zur Implementierung komponentenbasierter Software-Entwicklung auf Basis von Applikationsservern *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage Komponenten im Sinne einer Applikationsserver-orientierten Architektur zu entwerfen und zu implementieren, verteilte Transaktionsarchitekturen zu entwerfen und zu implementieren, verschiedene Frontend- und Backend-Architekturen zu entwickeln und zu implementieren *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen *Selbstständigkeit* Die Studierenden sind fähig selbständig komplexere Aufgabenstellungen im Sinne einer komponentenorientierten Software-Architektur zu modellieren und umzusetzen *[Eigenständigkeit/Verantwortung, 7]*				
4	**Inhalte*:*** Aufbau eines komponentenorientierten, TP-Monitor-basierten Applikationsservers Implementierung komplexer (Datenbank-) Anwendungen auf Basis der Java Persistence Architektur *Empfohlene Literaturangaben:* https://www.tutorialspoint.com/software_architecture_design/component_based_architecture.htm Syperski, C.: Component Software: Beyond Object-Oriented Programming (Addison-Wesley Component Software), 2011 Andresen, A.: Komponentenbasierte Softwareentwicklung mit MDA, UML 2 und XML.				

	Hanser, 2. Auflage, 2004,ISBN-13: 978-3446229150 Eilebrecht, K., Starke, G.: Patterns kompakt: Entwurfsmuster für effektive Software-Entwicklung. Spektrum Akademischer Verlag, 3. Auflage, 2010, ISBN-13: 978-3827425256 Erl, T.: SOA: Design Patterns. Prentice Hall International, 2008, ISBN-13: 978-0136135166Erl, T.: SOA: Entwurfsprinzipien für service-orientierte Architektur. Addison-Wesley, 2008, ISBN-13: 978-3827326515 Fowler, M. et al.: Patterns of Enterprise Application Architecture. mitp, 2003, ISBN-13: 978-3826613784 Gamma et al.: Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software. Addison-Wesley, Neuauflage, 2010, ISBN-13: 978-3827330437 Gharbi, M.: Basiswissen für Softwarearchitekten: Aus- und Weiterbildung nach iSAQB-Standard zum Certified Professional for Software Architecture - Foundation Level. dpunkt.verlag, 1. Auflage, 2012, ISBN-13: 978-3898647915 Wieken, J.-H.: SQL -Einstieg für Fortgeschrittene, Addison Wesley, 2008 Kroenke, D.M.; Auer, D.: Database Processing, Prentice Hall, 2010 Wehr, H., Müller, B.: Java Persistence API mit Hibernate, Addison Wesley, 2007Bauer, Chr.; King, G.: Hibernate in Action. Manning Pub., 2004 http://jbossts.blogspot.de/2014/01/narayana-transaction-analyser-100alpha1.htmlhttp://www.redhat.com/products/jbossenterprisemiddleware/data-grid/
5	**Teilnahmevoraussetzungen:** Teilnahmevoraussetzungen: Zulassung zum Master-Studiengang Business and Security Analysis MSc an der HS Albstadt Sigmaringen
6	**Prüfungsformen***:* Mündliche Prüfung 20 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der mündlichen Prüfung
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. J. Röhrle Dozenten: Prof. Dr. J. Röhrle
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.4 52400 – Financial Risks and Financial Management

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Modul: Financial Risks & Financial Management					
Kennnummer 52400	**Workload** 180 h	**Modulart** WPM	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** WS und SS

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_Business and Security Analytics_FINAL-1.docx		

1	**Lehrveranstaltung(en)** Vorlesung; Übungen & Fallstudien Financial Risks & Financial Management	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 120	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS Übungen / Fallstudien: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden: • sind mit zentralen Aspekten des Kapitalstrukturmanagements und der Ableitung der relevanten Kapitalkosten vertraut • kennen die Portfoliotheorie und das CAPM und deren Anwendungsgebiete im Risikomanagement und der Kapitalkostenableitung • kennen die wesentlichen Verfahren der Unternehmens- sowie der Anleihebewertung • sind mit den zentralen finanzwirtschaftlichen Risiken vertraut und kennen die gängigen Verfahren des Risikomanagements • kennen in Grundzügen das Wesen von Derivaten und deren Anwendungsmöglichkeiten im Management von finanzwirtschaftlichen Risiken *[Wissen, 7]* Lernergebnisbeschreibung einer bestimmten Kompetenz z.B. Fachwissen mit Niveaustufe /Niveaustufe wählen *Kompetenz Fertigkeiten* Die Studierenden: • können marktgestützt Kapitalkosten von Unternehmen ableiten • können die gängige Verfahren zur Unternehmensbewertung anwenden und selbständig Unternehmenswerte ableiten • können Anleihen bewerten • können die unterschiedlichen finanzwirtschaftlichen Risiken identifizieren und voneinander abgrenzen • können gängige Verfahren zum Management finanzwirtschaftlicher Risiken (Value at Risk, Hedging mittels Derivaten, etc.) anwenden • *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden können Fallstudien im Team bearbeiten und sind in der Lage die Teams selbst zu organisieren; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen *[Team-/Führungsfähigkeit, 7]* Die Studierenden beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden können im Rahmen von Fallstudien Problemstellungen des Finanz- und Risikomanagements selbständig erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen *[Eigenständigkeit/Verantwortung, 7]*				

	Durch die fortlaufende Vertiefung des Stoffes durch die selbständige Bearbeitung von Übungsaufgaben und Fallstduien, sind die Studierenden in der Lage, sich ein realistisches Bild ihrer eigenen Kompetenzentwicklung zu machen und entsprechend darauf zu reagieren. *[Lernkompetenz, 7]*
4	**Inhalte*:*** Frundlagen des Finanzmanagements, Finanzanalyse, Value Management und Unternehmenswert, Fremdkapitalmanagement, Finanzielle Risiken und Risikomanagement
	Empfohlene Literaturangaben: Becker, H. P.: Investition und Finanzierung –Grundlagen der betrieblichen Finanzwirtschaft, 7. Auflage, Springer Verlag, 2015, Brealey, R. A./ Myers, St. C., 2003, Principles of Corporate Finance, 7th. Ed., New York et. al. (Mc Graw Hill International Ed.), Elton, E., Gruber, M., Brown, S. und Goetzmann,W., 2002, Modern Portfolio Theory and Investment Analysis, 6. Aufl., John Wiley and SonsKruschwitz, L.;Husmann, S.: Finanzierung und Investition, 6. Auflage, Oldenbourg Verlag, 2009Hull, J.C.: Options, Futures, and Other Derivatives, 9th Edition, Pearson, 2015Higgins, R.: Analysis for Financial Management, 10thEdition, McGraw-Hill/Irwin, 2011Perridon, L.; Steiner, M.;Rathgeber, A.: Finanzwirtschaft der Unternehmung, 15. Auflage, Vahlen Verlag, 2009Zantow, R.;Dinauer, J.: Finanzwirtschaft der Unternehmens:Die Grundlagen des modernen Finanzmanagements, 3. Auflage,PearsonStudium, 2011
5	**Teilnahmevoraussetzungen:** Empfohlen: Grundlagen der Investition und Finanzierung, Grundlagen der Statistik
6	**Prüfungsformen***:* Klausur 90 min.
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Philipp Lindenmayer Dozenten: Prof. Dr. Philipp Lindenmayer
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.5 52500 – Innovation and Transfer Competence

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_Business and Security Analytics_FINAL-1.docx		

Modul: Innovation and Transfer Competence						
Kennnummer 52500	**Workload** 180	**Modulart** PM	**Studiensemester** 2	**Dauer** 1	**Häufigkeit** SS	
1	**Lehrveranstaltung(en)** a. 52305 In. and Transfer Competence b. 52320 Proj. In. and Transfer Competence	**Sprache** a.,b., deutsch oder englisch	**Kontakt-zeit** a. 15 b. 45	**Selbst-studium** 120	**Credits (ECTS)** 6	
2	**Lehrform(en) / SWS:** a. Vorlesung, Seminar b. Projektarbeit					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Methoden zur Integration einen betrieblichen Innovationsmangements in bestehende Betriebe *[Wissen, 7]* Planungs-, Organisations-und Qualitätsmanagementsmethoden aus Theorie und Praxis *[Wissen, 7]* *Kompetenz Fertigkeiten* Wissenschaftliche Grundlagen-und neuere Forschungsergebnisse erfassen, auf deren praktischen Einsatz hin prüfen, ergänzen und zum Einsatz bringen. *[Systemische Fertigkeiten, 7]* Zusammenhänge zwischen diversen Theorien und Konzepten zu sehen, diese zu umfassenderen integrierenden praxisorientierten Konzeptionen weiterzuentwickeln und in konkreten entwickelten Anwendungen zum Einsatz zu bringen *[Instrumentelle Fertigkeiten, 7]* Geschäftsideen entwickeln, diese bezügliche Realisierbarkeit prüfen und Strategien entwickeln, Forschungsergebnisse zu transferieren und als Innovation umzusetzen [Systemische Fertigkeiten, *7]* *Sozialkompetenz* Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. *[Team-/Führungsfähigkeit, 7]* *Selbstständigkeit* Sind in der Lage in einem konkurrierendem Kontext, eigene Ideen zu reflektieren, diese gegeben Falls anzupassen und durchzusetzen, oder sich Argumenten zu beugen und die Ideen der Wettbewerber zu akzeptieren *[Eigenständigkeit/Verantwortung, 7]*					
4	**Inhalte*:*** Vorlesung: - Ideenmanagement - Betriebliches Innovationsmanagement - Transfer Wissenschaft -Praxis Projekt					

	- Entwicklung eines ausführlichen Geschäftsszenarios, eines Qualitätsmanagementplans und einer Risikoabschätzung - Bestimmung, Suche und Auswahl der einzusetzenden wissenschaftlichen Forschungsergebnisse - Entwicklung einer Vermarktungsstrategie - Durchführen der Organisations-und Qualitätsplanung - Vornahme der Projektplanung (Aufgaben, Netzplan, Meilensteine) und Festlegung der Arbeitsverteilung (Rollen, Verantwortlichkeiten, Mitarbeit, Personalführung) - Leitung und Durchführung des Projekts - Betreiben des Projekt-und Risikomanagements - Durchführung von Produkttest, Endfertigung und Qualitätskontrolle
	Empfohlene Literaturangaben: Al-Laham, Andreas. Organisationales Wissensmanagement: Eine strategische Perspektive. Vahlen, 2016. Mertins, Kai, Ina Kohl, and Ronald Orth. "Ein Referenzmodell für Wissensmanagement." Wissensmanagement im Mittelstand. Springer Gabler, Berlin, Heidelberg, 2016. 31-40. Kamiske, Gerd F., and Jörg-Peter Brauer. Qualitätsmanagement von A-Z: Wichtige Begriffe des Qualitätsmanagements und ihre Bedeutung. Carl Hanser Verlag GmbH Co KG, 2016. Neumann, Alexander. Führungsorientiertes Qualitätsmanagement. Carl Hanser Verlag GmbH Co KG, 2017.
5	**Teilnahmevoraussetzungen:** Wissenschaftliches Arbeiten (DQR 6), Projektmanagement (DQR 5)
6	**Prüfungsformen***:* Praktische Arbeit (benotet) als Modulprüfung
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business und Security Analysis MSc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.6 52600 – Advanced Network and Internet Security

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_Business and Security Analytics_FINAL-1.docx		

Modul: Advanced Network and Internet Security (ANIS)						
Kennnummer 52600	**Workload** 180 h	**Modulart** WPM	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung, Seminar, Projekt	**Sprache** Englisch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 120	**Credits (ECTS)** 6	
2	**Lehrform(en) / SWS:** Vorlesung: 1 SWS Seminar: 1,5 SWS Projekt: 1,5 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen den aktuellen Forschungsstand ausgewählter Forschungsbereiche in der Netzwerksicherheit *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können Forschungsfragestellungen der Netzwerksicherheit mit geeigneten Mechanismen und Methoden in Verbindung setzen und diese zur Bearbeitung der Fragestellung anwenden [Instrumentelle Fertigkeiten, 7] Die Studierenden können eine Forschungsfragestellung bearbeiten und die erzielten Ergebnisse adäquat [Systemische Fertigkeiten, 7] *Sozialkompetenz* Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen *Selbstständigkeit* Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Systeme im Bereich Netzwerksicherheit entwickeln und bestehende Systeme bewerten erweitern und analysieren [Eigenständigkeit/Verantwortung, *7]*					
4	**Inhalte*:*** Die Vorlesung gliedert sich in drei Teile auf, die z.T. zeitlich überlappend durchgeführt werden: - Wiederholung und Vertiefung der Grundlagen und fortgeschrittenen Aspekte der Netzwerksicherheit. Dieser Teil wird im Rahmen einer Vorlesung absolviert und dient dazu Informatik Studenten ohne spezifischen IT Security Hintergrund die Grundlagen für die Bearbeitung des Referats und des Projekts zu vermitteln. - Ausarbeitung eines Referats über ein aktuelles Thema der Netzwerksicherheit (basierend auf aktuellen Konferenz- oder Journal Veröffentlichungen aus dem Bereich der Netzwerksicherheit). Dieser Teil dient dazu, an einem konkreten Beispiel den Aufbau einer wissenschaftlichen Arbeit zu erarbeiten und diese zu bewerten. Die Referate werden im Peer-Review Prozess von jeweils zwei Kommilitonen korrigiert und ähnlich zu einem Konferenzformat gehalten (1-tägige Blockveranstaltung). - Bearbeitung eines eigenen Projekts zu einer ausgewählten Forschungsfragestellung aus dem Bereich der Netzwerk- und Internetsicherheit. Dabei werden sowohl					

	Ingenieursmethoden als auch analytische Methoden verwendet um die Fragestellung zu beantworten. Die Projektbearbeitung schließt mit einem Vortrag über die Ergebnisse ab (erneut im Konferenz-Format als Blockveranstaltung). Hier sollen selbständig wissenschaftliche Fragestellungen bearbeitet werden. Beispiele für die zu behandelnden Themen • Sicherheit moderner Kommunikationsprotokolle (HTTP/2, QUIC, P2P Protokolle, etc.) • Aktuelle Angriffe gegen Kommunikationsprotokolle • Protokolle zur Erreichung spezifischer Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Anonymität, Pseudonymität) • Authentifikations- und Authorisierungsprotokolle • Sicherheit im industriellen Umfeld (Fertigung, Steuerung) • Analyse von Kommunikationsdaten zur Erkennung von Sicherheitsproblemen • Analyse verschlüsselter Verbindungen zur Klassifikation von Verkehr • Analyse von Log- Einträgen und anderweitig erfassten Ereignissen zur Erkennung und Klassifikation von Angriffen
	Empfohlene Literaturangaben: R. Anderson, Security Engineering, Wiley, 2009G. Schäfer, M. Roßberg, Netzssicherheit, dpunkt.verlag, 2014 Ausgewählte Literatur bekannter Top-Tier Konferenzen im Bereich Sicherheit und Netzwerksicherheit z.B. ACM CCS, Usenix Security, Defcon, Balckhat, etc.
5	**Teilnahmevoraussetzungen:** Bestandener Referat
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.7 52700 – Security Analytics

Studiengang: Business and Security Analytics **Semester**: WS 2020/21

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_Business and Security Analytics_FINAL-1.docx		

StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

<table>
<tr><td colspan="7">Modul: Security Analytics</td></tr>
<tr><td colspan="2">Kennnummer
52700</td><td>Workload
180</td><td>Modulart
PM</td><td colspan="2">Studiensemester
2</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
c. 52705 Security Analytics
d. 52720 Proj. Security Analytics</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
a. 30
b. 30</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, b. Projektarbeit</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den aktuellen Forschungsstand zu den Themenbereichen Security Analytics wie Malware Analytics or/and Security Network Package and Profess Analytics. [Wissen, 7]
Vertieftes Verstehen von Semantic Web -Technologien als Instrument für interoperable Wissensbeschreibung [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können den Analytischen Prozesse auf konkrete Aufgabenstellungen anwenden und mit spezifischen Methoden und Tools umsetzen. [Instrumentelle Fertigkeiten, 7]
Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen Security Analytics Prozess mit konkreter Aufgabenstellung entwickeln. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Sind in der Lage komplexe Aufgaben in einem Team zu bearbeiten, die Teamarbeit zu organisieren und die Rollen effektiv zu verteilen. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Sind in der Lage komplexe Aufgaben verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Definition und Begriffsklärung,
Security Analytics Use Cases,
Data Souesess und Methoden der Datensammlung ,
Real time Datensammeln,
Anwendung der Security Analytics Ergebnissen und ihr Impact,
Basic security analytics Costs,
Advanced persistent threats,
Security Analytics und Digitale Forensics,
Übersicht der security analytics tools and services, u.a.:
Blue Coat Security Analytics Platform,</td></tr>
</table>

	Lancope Stealth Watch System, Juniper Networks JSA Series Secure Analytics, EMC RSA Security Analytics NetWitness, FireEye Threat Analytics Platform, Arbor Networks Security Analytics, Click Security Click Commander, Hexis Cyber Solutions' NeatBeat MON, Sumo Logics' cloud service., Security Onion.
	Empfohlene Literaturangaben: Hitzler, P., Krötzsch, M., Rudolph, S., & Sure, Y. (2007). Semantic Web: Grundlagen. Springer-Verlag. Dengel, Andreas, ed. Semantische Technologien: Grundlagen. Konzepte. Anwendungen. Springer-Verlag, 2011. Ege, Börteçin, Bernhard Humm, and Anatol Reibold, eds. Corporate Semantic Web: Wie semantische Anwendungen in Unternehmen Nutzen stiften. Springer-Verlag, 2015.
5	**Teilnahmevoraussetzungen:** Grundkenntnisse in formalen Logiken (DQR 3), Kenntnisse in Web Technologien und auszeichnungssprachen (DQR 5)
6	**Prüfungsformen***:* Klausur 90 Min. (Modulprüfung), Praktische Arbeit (Projekt-Prüfung).
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur und die praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business und Security Analysis MSc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.3 3. Semester

5.3.1 60100 – Master-Thesis

Studiengang: Business and Security Analytics
StuPO-Version: 18.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Master-Thesis

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_Business and Security Analytics_FINAL-1.docx		

Kennnummer 60100	**Workload** 750 h	**Modulart** P	**Studiensemester** 3	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Projekt Master-Thesis	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** SWS / h	**Selbst-studium** 750 (Präsenz & Selbst-studium)	**Credits (ECTS)** 25

2	**Lehrform(en) / SWS:** Projekt, betreute selbständige wissenschaftliche Arbeit
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Lernergebnisbeschreibung einer bestimmten Kompetenz z.B. Fachwissen mit Niveaustufe /Niveaustufe wählen
	Kompetenz Fertigkeiten Mit der Master – Thesis zeigt der Student, dass er unter Anleitung selbständig umfangreiche wissenschaftliche Themen bearbeiten kann. Er wird praxisorientierte oder theoretische Themenstellungen nach wissenschaftlichen Kriterien analysieren, strukturieren und ergebnisorientiert bearbeiten. Die Master – Thesis dokumentiert seine Arbeit und erfüllt die Kriterien eines wissenschaftlichen Berichts. *[Systemische Fertigkeiten, 7]*
	Sozialkompetenz Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen
	Selbstständigkeit Master-Thesis ist das größte Projekt im gesamten Master-Studiums, das die Studierenden nachweislich selbständig und verantwortlich ausführen. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** abhängig von Thema und Inhalt der Master - Thesis
	Empfohlene Literaturangaben: Abhängig vom Thema und Inhalt der Master-Thesis
5	**Teilnahmevoraussetzungen:** Ggf. formal geregelt in der Prüfungsordnung
6	**Prüfungsformen***:* Master-Thesis (Ma.), benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Thesis (Positive Bewertung)

8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: abhängig vom Thema und Inhalt der Master-Thesis
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.3.2 60200 – Master-Thesis

Studiengang: Business and Security Analytics **Semester**: WS 2020/21
StuPO-Version: 18.2 **Letzte Bearbeitung**: 14.10.20

Modul: Mündliche Masterprüfung					
Kennnummer 60200	**Workload** 150 h	**Modulart** P	**Studiensemester** 3	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** 60210 Mastervortrag 60220 Masterprüfung	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** SWS / 0h	**Selbst-studium** 150 (Präsenz & Selbst-studium)	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Projekt, betreute selbständige wissenschaftliche Arbeit				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Lernergebnisbeschreibung einer bestimmten Kompetenz z.B. Fachwissen mit Niveaustufe /Niveaustufe wählen *Kompetenz Fertigkeiten* Mit dem Master – Vortrag sollen die Studierenden die Ergebnisse ihrer Tätigkeit in eine anschaulichen Art einem fachlich kompetenten Hörerkreis vermitteln. Die Verteidigung soll nicht nur eine Präsentation der wissenschaftlichen Ergebnisse der Masterarbeit, sondern auch eine Präsentation der Persönlichkeit des Vortragenden sein. *[Systemische Fertigkeiten, 7]* *Sozialkompetenz* Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen				

	Selbstständigkeit Insbesondere in der dem Vortrag folgenden Diskussion sollen die Studierenden Beweis von der Tiefgründigkeit und Sicherheit ihrer Kenntnisse abgeben. *[Lernkompetenz, 7]*
4	**Inhalte*:*** Ist abhängig vom Thema und Inhalt der Master - Thesis
	Empfohlene Literaturangaben: Anleitung zurwissenschaftlichen Arbeit. Vom Kandidaten selber vorzuschlagende vertiefende Literatur.
5	**Teilnahmevoraussetzungen:** Ggf. formal beschrieben in Prüfungsordnung
6	**Prüfungsformen***:* Referat 30 min., benotet Mündliche Prüfung 30 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Referat, Bestandene mündliche Prüfung
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: abhängig vom Thema und Inhalt der Master-Thesis
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul