fhwedel
UNIVERSITY OF APPLIED SCIENCES

Modulhandbuch
Master-Studiengang
IT-Sicherheit

Prüfungsordnung 19.0

Wedel, den 16. Dezember 2021

Teil I

Modulhandbuch

Kapitel I.1

Modulhandbuch

Modulverzeichnis nach Modulkürzel

M005 Funktionale Programmierung . . . 16
M006 Learning and Softcomputing . . . 20
M009 Workshop Cryptography . . . 24
M019 Security Engineering . . . 29
M027 Konzepte der Datenbanktechnologie . . . 34
M029 Berechenbarkeit und Verifikation . . . 38
M035 Distributed Systems . . . 47
M047 Projekt IT-Sicherheit . . . 51
M049 Security Management . . . 53
M050 Master-Thesis . . . 57
M058 Master-Kolloquium . . . 59
M120 Web- und Applikationssicherheit . . . 13
M121 Workshop Netzwerksicherheit . . . 43
M170 Seminar IT-Sicherheit . . . 32

Modulverzeichnis nach Modulbezeichnung

Berechenbarkeit und Verifikation 38

Distributed Systems 47

Funktionale Programmierung 16

Konzepte der Datenbanktechnologie 34

Learning and Softcomputing 20

Master-Kolloquium 59
Master-Thesis 57

Projekt IT-Sicherheit 51

Security Engineering 29
Security Management 53
Seminar IT-Sicherheit 32

Web- und Applikationssicherheit 13
Workshop Cryptography 24
Workshop Netzwerksicherheit 43

I.1.1 Erläuterungen zu den Modulbeschreibungen

Im Folgenden wird jedes Modul in tabellarischer Form beschrieben. Die Reihenfolge der Beschreibungen richtet sich nach der Abfolge im Curriculum.

Vor den Modulbeschreibungen sind zwei Verzeichnisse aufgeführt, die den direkten Zugriff auf einzelne Modulbeschreibungen unterstützen sollen. Ein Verzeichnis listet die Modulbeschreibungen nach Kürzel sortiert auf, das zweite Verzeichnis ist nach Modulbezeichnung alphabetisch sortiert.

Die folgenden Erläuterungen sollen die Interpretation der Angaben in einzelnen Tabellenfeldern erleichtern, indem sie die Annahmen darstellen, die beim Ausfüllen der Felder zugrunde gelegt wurden.

Angaben zum Modul

Modulkürzel:	FH-internes, bezogen auf den Studiengang eindeutiges Kürzel des Moduls
Modulbezeichnung:	Textuelle Kennzeichnung des Moduls
Lehrveranstaltungen:	Lehrveranstaltungen, die im Modul zusammen gefasst sind, mit dem FH-internen Kürzel der jeweiligen Leistung und ihrer Bezeichnung
Prüfung im Semester:	Auflistung der Semester, in denen nach Studienordnung erstmals Modulleistungen erbracht werden können
Modulverantwortliche(r):	Die strategischen Aufgaben des Modulverantwortlichen umfassen insbesondere: ▪ Synergetische Verwendung des Moduls auch in weiteren Studiengängen ▪ Entwicklung von Anstößen zur Weiterentwicklung der Moduls und seiner Bestandteile ▪ Qualitätsmanagement im Rahmen des Moduls (z. B. Relevanz, ECTS-Angemessenheit) ▪ Inhaltsübergreifende Prüfungstechnik. Die operativen Aufgaben des Modulverantwortlichen umfassen insbesondere: ▪ Koordination von Terminen in Vorlesungs- und Klausurplan ▪ Aufbau und Aktualisierung der Modul- und Vorlesungsbeschreibungen ▪ Zusammenführung der Klausurbestandteile, die Abwicklung der Klausur (inkl. Korrekturüberwachung bis hin zum Noteneintrag) in enger Zusammenarbeit mit den Lehrenden der Modulbestandteile

- Funktion als Ansprechpartner für Studierende des Moduls bei sämtlichen modulbezogenen Fragestellungen.

Zuordnung zum Curriculum:	Auflistung aller Studiengänge, in denen das Modul auftritt
Querweise:	Angabe, in welchem Zusammenhang das Modul zu anderen Modulen steht
SWS des Moduls:	Summe der SWS, die in allen Lehrveranstaltungen des Moduls anfallen
ECTS des Moduls:	Summe der ECTS-Punkte, die in allen Lehrveranstaltungen des Moduls erzielt werden können
Arbeitsaufwand:	Der Gesamtarbeitsaufwand in Stunden ergibt sich aus den ECTS-Punkten multipliziert mit 30 (Stunden). Der Zeitaufwand für das Eigenstudium ergibt sich, wenn vom Gesamtaufwand die Präsenzzeiten abgezogen werden. Diese ergeben sich wiederum aus den Semesterwochenstunden (SWS), die multipliziert mit 45 (Minuten) geteilt durch 60 die Präsenzzeit ergeben.
Voraussetzungen:	Module und Lehrveranstaltungen, die eine inhaltliche Grundlage für das jeweilige Modul darstellen. Bei Lehrveranstaltungen ist der Hinweis auf das jeweilige Modul enthalten, in dem die Lehrveranstaltung als Bestandteil auftritt.
Dauer:	Anzahl der Semester die benötigt werden, um das Modul abzuschließen
Häufigkeit:	Angabe, wie häufig ein Modul pro Studienjahr angeboten wird (jedes Semester bzw. jährlich)
Studien-/Prüfungsleistungen:	Auflistung aller Formen von Leistungsermittlung, die in den Veranstaltungen des Moduls auftreten
Sprache:	In der Regel werden die Lehrveranstaltungen aller Module auf Deutsch angeboten. Um Gaststudierenden unserer Partnerhochschulen, die nicht der deutschen Sprache mächtig sind, die Teilnahme an ausgewählten Lehrveranstaltungen zu ermöglichen, ist die Sprache in einigen Modulen als "deutsch/englisch" deklariert. Dieses wird den Partnerhochschulen mitgeteilt, damit sich die Interessenten für ihr Gastsemester entsprechende Veranstaltungen heraussuchen können.
Lernziele des:	Übergeordnete Zielsetzungen hinsichtlich der durch das Modul zu vermittelnden Kompetenzen und Fähigkeiten aggregierter Form

Angaben zu den Lehrveranstaltungen

Lehrveranstaltung:	Bezeichnung der Lehrveranstaltung, die im Modul enthalten ist
Dozent(en):	Namen der Dozenten, die die Lehrveranstaltung durchführen
Hörtermin:	Angabe des Semesters, in dem die Veranstaltung nach Studienordnung gehört werden sollte
Art:	Angabe, ob es sich um eine Pflicht- oder Wahlveranstaltung handelt
Lehrform:	Lehrform kann Vorlesung, Praktikum, Seminar, u.v.m. sein
Semesterwochenstunden:	Eine Semesterwochenstunde dauert 70 Minuten und entspicht einer Vorlesungseinheit
ECTS:	Angabe der ECTS-Punkte, die in dieser Lehrveranstaltung des Moduls erzielt werden können
Medienformen:	Auflistung der Medienform(en), die in der Veranstaltung eingesetzt werden
Lernziele:	Stichwortartige Nennung die zentralen Lernziele der Lehrveranstaltung
Inhalt:	Gliederungsartige Auflistung der wesentlichen Inhalte der Lehrveranstaltung
Literatur:	Auflistung der wesentlichen Quellen, die den Studierenden zur Vertiefung zu den Veranstaltungsinhalten empfohlen werden. Es wird keine vollständige Auflistung aller Quellen gegeben, die als Grundlage für die Veranstaltung dienen.

I.1.2 Web- und Applikationssicherheit

M120 Web- und Applikationssicherheit

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M120
Bezeichnung	Web- und Applikationssicherheit
Lehrveranstaltung(en)	M120a Web- und Applikationssicherheit
Verantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	IT-Sicherheit (Master)
Verwendbarkeit	Das Modul ergänzt die anderen Module im Bereich IT-Sicherheit.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Die Studierenden benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium erworben Fähigkeit zum analytischen Denken und zur Modellbildung. Weiterhin benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium Kenntnisse der Funktionsweise eines modernen Computers und Betriebssystems, der Netzwerktechnik und der Programmierung.
Dauer	1

Lernziele

Anwendungen werden heute in der Regel nicht mehr ausschließlich lokal auf dem Rechner des Anwenders ausgeführt, sondern greifen auf Server-Komponenten zurück oder laufen vollständig auf externen Servern. Hierdurch stellen sich besondere Anforderungen und Herausforderungen für die Sicherheit. Die Studierenden kennen die grundlegenden Konzepte der Web- und Applikationssicherheit sowie typische Schwachstellen. Die Studierenden sind in der Lage, Web-Applikationen entsprechend dem aktuellen State-of-the-Art bezüglich der Web-Sicherheit zu entwickeln. Sie sind auch in der Lage, webbasierte Client-Server-Architekturen in Hinblick auf ihre Sicherheit zu bewerten.

I.1.2.1 Web- und Applikationssicherheit

Lehrveranstaltung	Web- und Applikationssicherheit
Dozent(en)	Gerd Beuster
Hörtermin	2
Häufigkeit	jährlich
Lehrform	Workshop
Semesterwochenstunden	4
ECTS	5.0
Prüfungsform	Abnahme
Sprache	deutsch
Lehr- und Medienform(en)	E-Learning, interaktive Entwicklung und Diskussion von Modellen, Online-Aufbereitung, Softwaredemonstration, studentische Arbeit am Rechner

Lernziele

Die Studierenden ...

- kennen typische Schwachstellen und Sicherheitsprobleme von (Web-)Anwendungen und können die notwendigen Maßnahmen entwickeln und umsetzen, um diese zu vermeiden.
- sind in der Lage typische Schwachstellen bei selbstentwickelten (Web-)Anwendungen zu vermeiden.
- sind in der Lage, neben den technischen auch die relevanten organisatorischen Maßnahmen umzusetzen, um die Sicherheit von (Web-)Anwendungen zu gewährleisten.
- sind mit den relevanten Standards zur Applikationssicherheit vertraut und können diese anwenden.
- sind mit den relevanten Testmethodiken vertraut und sind in der Lage gängige Sicherheitsprobleme in Webanwendungen selbst zu identifizieren.

Inhalt

- Ursachen für unsichere Webanwendungen
- Einführung in die (Web-)Anwendungen
- Schwachstellen und Angriffe
- Technische Sicherheitsmaßnahmen
- Organisatorische (Web-)Anwendungssicherheit
- Prüfverfahren
- Relevante Standards

Literatur

- Matthias Rohr: Sicherheit von Webanwendungen in der Praxis, 2015, 78-3658038502

- Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2008, ISBN 978-0470068526
- David Rice, Geekonomics: The Real Cost of Insecure Software, 2010, David Rice, ISBN 978-0321735973
- Gary McGraw, Software Security: Building Security in (Addison-Wesley Software Security), 2006, 978-0321356703
- Joel Scambray, Vincent Liu, Caleb Sima: Hacking Exposed: Web Applications: Web Application Security Secrets and Solutions. 3. Auflage. Verlag Mcgraw-Hill Professional, 2010, ISBN 978-0-07-174064-7.
- William Stallings, Lawrie Brown: Computer Security - Principles and Practice, Third Edition, Pearson, 2015
- Abhinav Singh: Metasploit Penetration Testing Cookbook, Packt Publishing, 2012-06-22
- Georgia Weidmanf: Penetration Testing - A Hands-On Introduction to Hacking, No Starch Press, 2014
- Vivek Ramachandran, Cameron Buchanan: Kali Linux - Wireless Penetration Testing Beginners Guide, Packt Publishing, 2015
- Kevin Cardwell: Building Virtual Pentesting Labs for Advanced Penetration Testing, Packt Publishing, 2014-07-19
- Aaron Johns: Mastering Wireless Penetration Testing for Highly Secured Environments, Packt Publishing, 2015
- Joseph Muniz, Aamir Lakhani: Web Penetration Testing with Kali Linux, Packt Publishing, 2013

I.1.3 Funktionale Programmierung

M005 Funktionale Programmierung

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M005
Bezeichnung	Funktionale Programmierung
Lehrveranstaltung(en)	M005a Funktionale Programmierung M005b Übg. Funktionale Programmierung
Verantwortliche(r)	Priv.-Doz. Dr. Frank Huch
Zuordnung zum Curriculum	IT-Sicherheit (Master) Informatik (Master)
Verwendbarkeit	Das Modul kann sinnvoll im Modul "Methoden der Künstlichen Intelligenz", in Projekten und der Master-Thesis genutzt werden.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Voraussetzungen sind Kenntnisse und praktische Erfahrungen in höheren Programmiersprachen, insbesondere mit getypten Sprachen. Außerdem werden Kenntnisse über Diskrete Mathematik und algebraische Strukturen erwartet. Elementares Wissen über Komplexitätstheorie wird ebenfalls vorausgesetzt.
Dauer	1

Lernziele

In diesem Modul werden fortgeschrittenen Techniken der funktionalen Programmierung am Beispiel der Sprache Haskell behandelt. Hierzu gehören der Umgang mit Funktionen höherer Ordnung, das Arbeiten mit generischen Datentypen und mit Typklassen, und mit Monaden und Arrows. Es werden beispielhaft eingebettete problemspezifische Sprachen (EDSL) vorgestellt. Dieses Modul soll außerdem die Abstraktion, die Modellbildung stärken und das aus der Mathematik bekannte präzise Arbeiten auf die Software-Entwicklung übertragen. Die Studierenden erfassen, warum funktionale Programmierung gegenüber anderen Programmieransätzen die IT-Sicherheit erhöhen kann, da sie typische Angriffslücken grundsätzlich vermeidet. Die Studierenden lernen, warum Kernelemente funktionaler Programmierung, insbesondere die Seiteneffektfreiheit und die starke Typisierung, besonders geeignet sind, Sicherheitsaspekte von Software zu gewährleisten und nachzuweisen.

I.1.3.1 Funktionale Programmierung

Lehrveranstaltung	Funktionale Programmierung
Dozent(en)	Uwe Schmidt
Hörtermin	2
Häufigkeit	jährlich
Lehrform	Vorlesung
Semesterwochenstunden	2
ECTS	2.0
Prüfungsform	Klausur / Mündliche Prüfung
Sprache	deutsch
Lehr- und Medienform(en)	Softwaredemonstration

Lernziele

Die Studierenden ...

- lernen fortgeschrittene Techniken der funktionalen Programmierung am Beispiel der Sprache Haskell kennen.
- können mit Funktionen höherer Ordnung, mit generischen Datentypen und Typklassen, mit Funktoren, Monaden, Monoiden und weiteren mathematischen Strukturen umgehen.
- lernen die Software-Realisierung mit eingebetteten problemspezifischen Sprachen kennen.
- stärken die Fähigkeiten in der Modellbildung und Abstraktion.
- lernen die Bezüge zwischen Mathematik und funktionaler Programmierung kennen.
- kennen die Vor- und Nachteile des funktionalen Paradigmas für Anwendungen der IT-Sicherheit.

Inhalt

- Einleitung
  - Grundlegende Konzepte
  - Syntax von Haskell
- Datentypen
  - Einfache Datentypen
  - Produkt- und Summen-Datentypen
  - Listen
  - Funktionen höherer Ordnung für Listen
- Typcheck
- Korrektheitsargumentationen
- Rekursive Datenstrukturen

  - Bäume
- Bedarfsauswertung
  - Unendliche Strukturen
- Funktoren und Monaden
  - Maybe- und Listen-Monade
  - Zustands-Monade und Ein- und Ausgabe
  - weitere Varianten von Monaden
- Fallstudien
  - Eingebettete problemspezifische Sprachen
  - Monadische Parser
- Parallele und nebenläufige Programmierung
- Testen

Literatur

- Uwe Schmidt:
  Funktionale Programmierung,
  Vorlesungsunterlagen im Web: `http://www.fh-wedel.de/si/vorlesungen/fp/fp.html`
- Bird, Richard:
  Introduction to Functional Programming using Haskell,
  2nd Edition Prentice Hall, New Jersey, 1998, ISBN: 0-13-484346-0
- Graham Hutton: Programming in Haskell, Cambridge University Press, 2007, ISBN: 978-0-521-69269-4

I.1.3.2 Übg. Funktionale Programmierung

Lehrveranstaltung	Übg. Funktionale Programmierung
Dozent(en)	Uwe Schmidt
Hörtermin	2
Häufigkeit	jährlich
Lehrform	Übung/Praktikum/Planspiel
Semesterwochenstunden	2
ECTS	3.0
Prüfungsform	Abnahme
Sprache	deutsch
Lehr- und Medienform(en)	studentische Arbeit am Rechner

Lernziele

Ziel der Übung ist das Erlernen des praktischen Anwenden der Methoden und Konzepte aus der Vorlesung.

Inhalt

Praktische Übungen über die Themen

- Rekursion,
- Typisierung,
- Listen und Tuple,
- Funktionen als Daten,
- Funktoren und Monaden,
- Ein-und Ausgabe.

Literatur

- Uwe Schmidt:
  Funktionale Programmierung,
  Vorlesungsunterlagen im Web: `http://www.fh-wedel.de/si/vorlesungen/fp/fp.html`
- Bird, Richard:
  Introduction to Functional Programming using Haskell,
  2nd Edition Prentice Hall, New Jersey, 1998, ISBN: 0-13-484346-0
- Graham Hutton: Programming in Haskell, Cambridge University Press, 2007, ISBN: 978-0-521-69269-4

I.1.4 Learning and Softcomputing

M006 Learning and Softcomputing

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M006
Bezeichnung	Learning and Softcomputing
Lehrveranstaltung(en)	M006a Learning & Softcomputing
Verantwortliche(r)	Prof. Dr. Ulrich Hoffmann
Zuordnung zum Curriculum	Data Science & Artificial Intelligence (Master) IT-Sicherheit (Master) Informatik (Master) Wirtschaftsinformatik/IT-Management (Master)
Verwendbarkeit	Das Modul ist sinnvoll mit dem Modul "Robotics" und den grundlegenden Modulen "Einführung in die Robotik" und "Bildbearbeitung und -analyse" kombinierbar. Zudem bietet sich ein Zusammenspiel in Richtung Data Sciences an, wenn es mit den grundlegenden Modulen "Deskriptive Statistik & Grundlagen der Linearen Algebra", "Induktive Statistik" und im Master mit den Modulen "Business Intelligence", "Empirische Forschungs- und Analysemethoden" und "Entscheidungsunterstützung" kombiniert wird.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Voraussetzungen dieses Moduls sind Kenntnisse und praktische Erfahrungen in höheren Programmiersprachen. Außerdem werden mathematische Grundkenntnisse und Kenntnisse der Stochastik erwartet.
Dauer	1

Lernziele

Studierende erwerben Kenntnisse im Bereich des maschinellen Lernens. Sie beherrschen die wesentlichen Techniken, mit deren Hilfe Computersysteme Klassifizierungen und Bewertungen durchführen, und sie können sie nach Einsatzgebiet und Güte bewerten und beurteilen. Sie kennen die Herausforderungen die beim Parametrieren von überwachtem Lernenverfahren bedeutsam sind und können sie praktisch anwenden. Sie sind mit wesentlichen Funktionalitäten gängiger Machine-Learning-Bibliotheken vertraut. Sie sind in der Lage eigenständig Aufgaben des maschinenen Lernens zu analysieren, geeignete Methoden auszuwählen und umzusetzen.

Im praktischen Teil erwerben sie zusätzlich die Kompetenz arbeitsteilig in einer kleinen Arbeitsgruppe wissenschaftlich, selbständig an einer umfangreichen Aufgabe Kenntnisse zusammenzutragen und Lösungen zu erarbeiten sowie diese verständlich und strukturiert zu präsentieren. Darüber hinaus erwerben oder vertiefen sie ihr Fachwissen über das Thema der zu bearbeitenden Aufgabe des maschinellen Lernens, z.B. Bildverarbeitung, IT-Sicherheit, E-Commerce oder Betriebswirtschaftslehre.

I.1.4.1 Learning & Softcomputing

Lehrveranstaltung	Learning & Softcomputing
Dozent(en)	Ulrich Hoffmann
Hörtermin	2
Häufigkeit	jährlich
Lehrform	mehrere Veranstaltungsarten
Semesterwochenstunden	4
ECTS	5.0
Prüfungsform	Assessment
Sprache	deutsch
Lehr- und Medienform(en)	

Lernziele

Die Studierenden ...

- besitzen grundlegende Kompetenz zum Verständnis für lernfähige, fehlertolerante Problemlösungsansätze.
- haben die Fähigkeit zur Erkennung und Unterscheidung verschiedener maschineller Lernverfahren und Verarbeitungskonzepte.
- haben grundlegendes Verständnis der Themenkomplex Künstlicher Neuronaler Netze (KNN) sowie der Support Vector Machines (SVM)
- besitzen die Fähigkeit unterschiedlichen Ansätze überwachter und unüberwachter Klassifikationsverfahren und ihre mathematischen Hintergründe zu durchdringen.
- haben die Fähigkeit, eine beispielhafte Implementierung dargestellten theoretischen Konzepten im Rahmen selbständiger, gruppenorientierter Projektarbeit gezielt und strukturiert umzusetzen.
- besitzen die Fähigkeit die von ihnen im Rahmen der Projektarbeit erarbeiteten Sachverhalte zu kondensieren und in angemessenen Vortragsstil und geeigneter Präsentationstechniken nachvollziehbar dazustellen. In freier Diskussion können sie sich über komplexe wissenschaftlichen Sachverhalts auseinandersetzen.
- besitzen vertiefte Kenntnisse des Themas der konkret bearbeiteten Machine-Learning-Aufgabe, also etwa zu Bildverarbeitung, IT-Sicherheit, E-Commerce oder Betriebswirtschaftslehre.

Inhalt

- Einführung, Motivation
- Maschinelles Lernen
- Das Konzept der Neuronalen Netze
  - Grundprinzip
  - Arten von Neuronalen Netzen
  - Einlagige Neuronale Netze

  - Mehrlagige Netze
  - Ein Lernverfahren: Backpropagation
- Das Konzept der Support Vector Machines
  - Grundlagen und Eigenschaften
  - Klassifikation durch Hyperebenen
  - Der Kernel-Trick
  - Aspekte der Implementierung von SVM
- Praktische Projektarbeit in Gruppen zur eigenständigen Implementierung und Untersuchung eines ausgewählten Themenkomplexes.
- Regelmäßige Diskussion der Ergebnisse der Projektarbeit und gruppenweise Abschlusspräsentation.

Literatur

- Kecman: Learning and Softcomputing,
  MIT Press, 2001
- Nauck, Klawonn: Neuronale Netze und Fuzzy-Systeme, R. Kruse,
  Vieweg 1996
- Bishop: Neural Networks for Pattern Recognition,
  Oxford Press 1995
- Sutton, Barto: Reinforcement Learning: An Introduction,
  MIT Press, Cambridge, MA, 1998
- Christianini, Shawe-Taylor: Support Vector Machines, N.,
  Cambridge Press, 2000
- Brause: Neuronale Netze,
  Teubner, 1991

I.1.5 Workshop Cryptography

M009 Workshop Cryptography

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M009
Bezeichnung	Workshop Cryptography
Lehrveranstaltung(en)	M009a Workshop Cryptography
Verantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	IT Engineering (Master) IT-Sicherheit (Master) Informatik (Master)
Verwendbarkeit	Für dieses Modul sind Grundkenntnisse der diskreten Mathematik erforderlich. Die Studierenden erwerben fortgeschrittene Kenntnisse über die mathematischen Grundlagen der Kryptographie und deren praktische Anwendung. Diese Kenntnisse können in allen Bereichen eingesetzt werden, in denen kryptographische Methoden verwendet werden.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Die Studierenden benötigen das Wissen über diskrete Mathematik, das typischerweise in einem Bachelor-Studiengang in Informatik oder einem ähnlichen Bereich erworben wird. Die Studierenden müssen mit den gängigen Internet-Protokollen vertraut sein. Die Studierenden müssen über einige Grundkenntnisse in der Programmierung verfügen.
Dauer	1

Lernziele

Im Kryptographie-Workshop erwerben die Studierenden Kenntnisse über die mathematischen Grundlagen der Kryptographie und deren praktische Anwendung. Nach Abschluss des Kurses sind die Studierenden in der Lage, kryptographische Verfahren im Kontext sicherer IT-Systeme einzusetzen und den Einsatz kryptographischer Verfahren in bestehenden Systemen zu evaluieren.

Dies umfasst sowohl software- als auch hardwarebasierte Kryptographie. Ein Schwerpunkt liegt auf der Kryptographie, die im Internet und für den E-Commerce eingesetzt wird. Die Studierenden wissen, wie die Vertraulichkeit und Integrität von persönlichen Daten und

Geschäftsdaten mit kryptographischen Mitteln sichergestellt werden kann. Basierend auf kryptographischen Systemen der realen Welt lernten die Studierenden, dass bei der Implementierung und Anwendung kryptographischer Methoden viele Nebenbedingungen berücksichtigt werden müssen.

I.1.5.1 Workshop Cryptography

Lehrveranstaltung	Workshop Cryptography
Dozent(en)	Gerd Beuster
Hörtermin	2
Häufigkeit	jährlich
Lehrform	Workshop
Semesterwochenstunden	4
ECTS	5.0
Prüfungsform	Abnahme
Sprache	english
Lehr- und Medienform(en)	E-Learning, Softwaredemonstration, studentische Arbeit am Rechner

Lernziele

Nach Abschluss des Moduls sind die Studierenden in der Lage, ...

- Sicherheitswerkzeuge als wesentlichen Baustein moderner Informations- und Kommunikationssysteme zu verwenden.
- ihr Wissen über alle relevanten Aspekte der Daten-, Netzwerk- und Websicherheit anzuwenden.
- die Anwendung kryptographischer Methoden, insbesondere zur Authentifizierung, Verschlüsselung und Integritätserhaltung zu betrachten.
- die algorithmischen Stärken und Schwächen der kryptographischen Verfahren zu bewerten.
- kryptographische Protokolle zu bewerten und zu implementieren, insbesondere für die Authentifizierung im E-Commerce.
- alle für die Implementierung und Anwendung kryptographischer Methoden relevanten Nebenbedingungen zu berücksichtigen.
- die Qualität von Zufallszahlengeneratoren zu beurteilen.
- die Eignung von Software- und Hardware-Kryptographie für eine bestimmte Aufgabe abzuschätzen.

Inhalt

- Theorie der Kryptographie
  - Semantische Sicherheit
  - Unbrechbare Verschlüsselung und One Time Pad
  - Diffusion und Verwirrung
- Klassische Kryptographie
  - Substitution und Transposition
  - Affine Verschlüsselung

  - Rotormaschinen
- Moderne Kryptographie
  - Stream- und Block-Chiffren
  - DES und GOST
  - AES
- Blockchiffrierung Betriebsarten
  - ECB, CBC, CTR, AES-GCM
- Zufallszahlengeneratoren
  - TRNG und PRNG
  - Voraussetzungen für CSPRNG
  - PRNG auf der Grundlage mathematischer Probleme
    * Blum-Blum-Shub
- Hashing
  - Hashing-Algorithmen
    * SHA 2
    * Keccak
  - Nachrichten-Authentifizierung
    * CMAC und HMAC
- Asymmetrische Kryptographie
  - Diffie-Hellman
  - RSA
  - Elliptische Kurven
  - Asymmetrische Verschlüsselung und digitale Signaturen
- Praktische Kryptographie: PGP und SSL
- Hardware-Kryptographie
  - Trusted Computing
  - Smartcards
  - Differenzleistungsanalyse

Literatur

- Stallings, William: Cryptography and Network Security : Principles and Practice. 7. Edition. London, UK: Pearson, 2017.
- Ferguson, Niels; Schneier, Bruce; Kohno, Tadayoshi: Cryptography Engineering : Design Principles and Practical Applications. Indianapolis (IN), USA: Wiley Publishing, 2010.

- Menezes, Alfred J.;van Oorschot, Paul C.; Vanstone, Scott A.: Handbook of Applied Cryptography. Boca Raton (FL), USA: CRC Press, 1996.
- Douglas R. Stinson: Cryptography : Theory and Practice. 3. Edition. Boca Raton (FL), USA: CRC Press, 2005.
- Lawrence C. Washington: Elliptic Curves : Number Theory and Cryptography. 2. Edition. Boca Raton (FL), USA: CRC Press, 2008.
- Joshua Davies: Implementing SSL/TLS Using Cryptography and PKI. Indianapolis (IN), USA: Wiley Publishing, 2011.
- Katz, Jonathan; Lindell, Yehuda: Introduction to Modern Cryptography. Boca Raton (FL), USA: CRC Press, 2007.
- Swenson, Christopher: Modern Cryptanalysis : Techniques for Advanced Code Breaking. Indianapolis (IN), USA: Wiley Publishing, 2008.
- Mao, Wenbo: Modern Cryptography: Theory and Practice, Upper Saddle River (NJ), USA: Prentice Hall, 2003.

I.1.6 Security Engineering

M019 Security Engineering

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M019
Bezeichnung	Security Engineering
Lehrveranstaltung(en)	M019a Security Engineering
Verantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	IT Engineering (Master) IT-Sicherheit (Master)
Verwendbarkeit	Das Modul erfordert Grundkenntnisse in den Bereichen Computerarchitektur, Betriebssysteme, Computernetzwerke und Programmierung. Die in diesem Modul erworbenen Fähigkeiten sind auf alle Aufgaben anwendbar, die Software und Sicherheitstechnik betreffen.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Die Studierenden müssen in der Lage sein, analytisch zu denken und formale Methoden zu entwickeln. Diese Fähigkeiten werden in der Regel in einem Bachelor-Studiengang in Informatik oder einem ähnlichen Bereich erworben. Darüber hinaus müssen die Studierenden die allgemeinen Prinzipien moderner Computer und Betriebssysteme, Netzwerktechnologie und Programmierung kennen.
Dauer	1

Lernziele

Nach Abschluss des Moduls sind die Studierenden in der Lage, die Sicherheit bestehender IT-Systeme zu bewerten und neue, sichere IT-Systeme zu entwerfen und zu implementieren. Dieses Modul konzentriert sich auf die ingenieurwissenschaftlichen Aspekte der IT-Sicherheit. Nach Abschluss des Moduls kennen die Studierenden den Stand der Technik in den Bereichen sichere Software, sichere Hardware, Netzwerksicherheit und physische Sicherheit. Die Studierenden sind in der Lage, Systeme zu entwerfen, die eine angemessene Sicherheit sowohl für persönliche als auch für geschäftliche Daten bieten. Sie kennen Methoden der Software- und Hardware-Analyse und sind in der Lage, technische Analysen von Sicherheitsvorfällen vorzunehmen.

I.1.6.1 Security Engineering

Lehrveranstaltung	Security Engineering
Dozent(en)	Gerd Beuster
Hörtermin	2
Häufigkeit	jährlich
Lehrform	Vorlesung mit integrierter Übung/Workshop/Assigm.
Semesterwochenstunden	4
ECTS	5.0
Prüfungsform	Klausur / Mündliche Prüfung
Sprache	english
Lehr- und Medienform(en)	E-Learning, interaktive Entwicklung und Diskussion von Modellen, Softwaredemonstration, studentische Arbeit am Rechner

Lernziele

Nach Abschluss des Moduls sind die Studierenden in der Lage, ...

- die grundlegenden Konzepte der IT-Sicherheit anzuwenden.
- Sicherheitsanforderungen für Software zu definieren und zu überprüfe.
- sichere Software zu entwickeln und zu evaluieren.
- die Sicherheit von Hardware-Komponenten zu beurteilen und evaluieren.
- die Sicherheit von Computernetzwerken zu bewerten.
- sichere Computernetzwerke zu entwerfen.

Inhalt

- Grundbegriffe der IT-Sicherheit
- Sicherheitsmodellierung
- Sicherheitsadministration und physische Sicherheit
- Sicherheit des Betriebssystems
- Identitätsmanagement, Zugriffskontrolle, Security Tokens, Biometrie
- IoT-Sicherheit
- Cloud-Sicherheit
- Reverse Engineering
- IT-Forensik
- Sicherheitsprotokolle
- Methoden der Entwicklung sicherer Software
- Typische Angriffe auf Softwaresysteme

- Verteilte Systeme / Netzwerksicherheit
- Sichere Hardware

Literatur

- Allen, Julia H.; Barnum, Sean; Ellison, Robert J.; McGraw, Gary; Mead, Nancy R.: Software Security Engineering : A Guide for Project Managers. Bosten (MA), USA: Addison Wesley, 2008.
- Anderson, Ross J.: Security Engineering : A Guide to Building Dependable Distributed Systems. 3. Edition. Hoboken (NJ), USA: Wiley & Sons, 2021.
- Graves, Michael W.: Digitial Archaeology : The Art and Science of Digital Forensics. Bosten (MA), USA: Addison Wesley, 2014.
- Johansen, Gerard: Digital Forensics and Incident Response : An intelligent way to respond to attacks. Birmingham, UK: Packt, 2017.
- Oettinger, William: Learn Computer Forensics : A beginner's guide to searching, analyzing, and securing digital evidence. Packt Publishing. Birmingham, UK, 2020.
- Pfleeger, Charls P.;Pfleeger, Shari Lawrence: Security in Computing. 5. Edition. Hoboken (NJ), USA: Prentice Hall, 2015.
- Shimeall, Timothy J.; Spring, Jonathan M.: Introduction to Information Security : A Strategic-based Approach. Amsterdam, NL: Elsevier Syngress, 2013.
- Stallings, William: Computer Security : Principles and Practice. 4. Edition. London, UK: Pearson Education, 2017.
- Weidman, Georgia: Penetration Testing : A Hands-On Introduction to Hacking. San Francisco (CA), USA: No Starch Press, 2014

I.1.7 Seminar IT-Sicherheit

M170 Seminar IT-Sicherheit

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M170
Bezeichnung	Seminar IT-Sicherheit
Lehrveranstaltung(en)	M170a Seminar IT-Sicherheit
Verantwortliche(r)	jeweiliger Dozent
Zuordnung zum Curriculum	IT-Sicherheit (Master)
Verwendbarkeit	Die Fähigkeit, theoriegestützt zu arbeiten, wird in der Master-Thesis benötigt.
Semesterwochenstunden	2
ECTS	5.0
Voraussetzungen	Keine
Dauer	1

Lernziele

Nach dem Seminar sind die Studierenden in der Lage, anspruchsvolle Themen eigenständig stärker theorieorientiert zu strukturieren und ihre Ausarbeitungen nach wissenschaftlichen Standards zu konzipieren. Im obligatorischen Vortrag können sie ihre Arbeitsergebnisse fundiert darlegen und im Diskurs kritisch diskutieren.

I.1.7.1 Seminar IT-Sicherheit

Lehrveranstaltung	Seminar IT-Sicherheit
Dozent(en)	jeweiliger Dozent
Hörtermin	2
Häufigkeit	jährlich
Lehrform	Seminar
Semesterwochenstunden	2
ECTS	5.0
Prüfungsform	Schriftl. Ausarbeitung (ggf. mit Präsentation)
Sprache	deutsch
Lehr- und Medienform(en)	Beamerpräsentation, Handout, interaktive Entwicklung und Diskussion von Modellen, Online-Aufbereitung, Softwaredemonstration, studentische Arbeit am Rechner, Tafel

Lernziele

Die Studierenden ...

- sind in der Lage, eine wissenschaftliche fundierte Lösung für theoretische und/oder praktische Problemstellungen primär aus dem Themengebiet sowie ähnlichen Gebieten zu entwickeln.
- zeigen eine verbesserte Problemlösungstechnik, sicherere Verwendung von Termini, präzise Strukturierung im Aufbau schriftlicher Arbeiten und Einhalten der Formalia.
- zeigen eine auf Masterniveau angemessene Vortragstechnik im Rahmen der Präsentation der Ergebnisse.

Inhalt

Fachvorträge mit anschließender Gruppendiskussion.

Literatur

Recherche nach aufgabenbezogener Literatur, teilweise aufgabenspezifische Vorgabe einzelner Literaturquellen.

I.1.8 Konzepte der Datenbanktechnologie

M027 Konzepte der Datenbanktechnologie

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M027
Bezeichnung	Konzepte der Datenbanktechnologie
Lehrveranstaltung(en)	M027a Konzepte der Datenbanktechnologie M027b Übg. Konzepte der Datenbanktechnologie
Verantwortliche(r)	Dr. Michael Predeschly
Zuordnung zum Curriculum	Data Science & Artificial Intelligence (Master) E-Commerce (Master) IT-Sicherheit (Master) Informatik (Master) Wirtschaftsinformatik/IT-Management (Master)
Verwendbarkeit	Das Modul ist sinnvoll im Datenbanken-Curriculum zusammen mit den grundlegenden Modulen "Einführung in Datenbanken" und "Datenbanktheorie und -implementierung" aber auch den Programmiereinführungsmodulen ("Einführung in die Programmierung", "Programmstrukturen 1") zu kombinieren. Auch eine Kombination mit dem grundlegenden Modul "Systemmodellierung" ist ratsam.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Das Modul setzt solide Kenntnisse der Funktionsweise und des Aufbaus relationaler Datenbankmanagementsysteme voraus. Der praktische Anteil erfordert fortgeschrittene Fähigkeiten der objektorientierten Programmierung.
Dauer	1

Lernziele

Nach Abschluss des Moduls besitzen die Studierenden fortgeschrittene Kenntnisse über Datenbanksysteme. Sie verfügen dabei über Wissen über relationaler Datenbanksysteme und über Datenbanksysteme, die auf alternativen Ansätzen (objekt-orientiert, objekt-relational, NoSQL, u., a.) basieren. Sie können deren Vor- und Nachteile abwägen. Die Studierenden sind in der Lage, sich kritisch mit den Möglichkeiten moderner Datenbanksysteme auseinanderzusetzen, diese geeignet einzuschätzen und praxisgerecht anzuwenden.

I.1.8.1 Konzepte der Datenbanktechnologie

Lehrveranstaltung	Konzepte der Datenbanktechnologie
Dozent(en)	Michael Predeschly
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Vorlesung
Semesterwochenstunden	2
ECTS	3.0
Prüfungsform	Klausur / Mündliche Prüfung
Sprache	deutsch
Lehr- und Medienform(en)	Beamerpräsentation, E-Learning, Gastreferenten, Online-Aufbereitung, Softwaredemonstration, Tafel, Tutorien

Lernziele

Die Studierenden erlangen die ...

- Kenntnis, der für die Implementierung von Datenbanksystemen wichtigen Architekturprinzipien, Datenstrukturen und Algorithmen und damit Kenntnis des Aufbaus und der internen Arbeit eines großen komplexen Softwaresystems.
- Fähigkeit, die Arbeitsweise von Datenbanksystemen zu optimieren bzw. selbst Architekturen für große komplexe Softwaresysteme zu entwerfen.
- Fähigkeiten eines Datenbankadministrators für Datenbanksysteme.
- Konzepte und Techniken des Datenschutzes, als auch der Datensicherheit

Inhalt

- Grundlagen Datenbanksysteme
  - Persistenz
  - Transaktionen
  - 2PL
  - Datenschutz und Datensicherheit
- Objekt-relationales Mapping
  - Java Persistence API (JPA)
- NoSQL-Datenbanksysteme
  - Verteilte Wert/Schlüssel-Speicher
  - Dokumentendatenbanken
  - Graph-Datenbanken
- Verteilung von Daten

Literatur

- KEMPER, Alfons; EICKLER, Andre:
  Datenbanksysteme - Eine Einführung. Oldenbourg Verlag, 2004
- KEITH, Mike; SCHINCARIOL, Merrik:
  Pro JPA 2 - Mastering the Java Persistence API. APress, 2009
- BAUER, Christian; KING, Gavin:
  Java Persistence with Hibernate,
  Manning, Greenwich, 2007
- SQL- & NoSQL-Datenbanken – Andreas Meier, Michael Kaufmann; eXamen.press Springer Vieweg
- Sieben Wochen, sieben Datenbanken – Eric Redmond, Jim R. Wilson; O'Reilly
- NoSQL for Dummies, Adam Fowler; For Dummies-Verlag
- div. Konferenzbeiträge und Forschungsarbeiten zu moderneren Entwicklungen der Datenbanktechnologie

I.1.8.2 Übg. Konzepte der Datenbanktechnologie

Lehrveranstaltung	Übg. Konzepte der Datenbanktechnologie
Dozent(en)	Michael Predeschly
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Übung/Praktikum/Planspiel
Semesterwochenstunden	2
ECTS	2.0
Prüfungsform	Abnahme
Sprache	deutsch
Lehr- und Medienform(en)	Beamerpräsentation, E-Learning, Gastreferenten, Online-Aufbereitung, Tafel

Lernziele

Studierende ...

- beherrschen die Fähigkeit Objektrelationales Mapping anzuwenden bzw. in Betrieb zu nehmen und es zur Lösung von Problemen einzusetzen.
- sind mit den praktisch auftretenden Schwierigkeiten vertraut und können sie systematisch überwinden.
- sind in der Lage eine NoSQL-Datenbank einzurichten, sie mit Daten zu füllen und anfragen an sie zu stellen

Inhalt

Vorlesungsbegleitende praktische Übungen zu Objektrelationalem Mapping und anderen alternativen Persistenzansätzen.

Erstellung einer NoSQL-Datenbank mit einem kompletten CRUD-Zyklus.

Literatur

- siehe Vorlesung
- diverse Online-Quellen

I.1.9 Berechenbarkeit und Verifikation

M029 Berechenbarkeit und Verifikation

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M029
Bezeichnung	Berechenbarkeit und Verifikation
Lehrveranstaltung(en)	M029a Berechenbarkeit und Komplexität M029a Formale Spezifikation und Verifikation
Verantwortliche(r)	Prof. Dr. Sebastian Iwanowski
Zuordnung zum Curriculum	IT-Sicherheit (Master) Informatik (Master)
Verwendbarkeit	Das Modul gibt eine Vertiefung der wissenschaftlichen Grundlagen des Informatikstudiums. Es ergänzt auf diese Weise das grundlegendere und anwendungsbezogenere Modul "Algorithmics", setzt dieses aber nicht voraus. Für IT-Sicherheitsapplikationen liefert es die theoretische Grundlage.
Semesterwochenstunden	6
ECTS	5.0
Voraussetzungen	Vorausgesetzt wird ein sehr gutes mathematisches Grundwissen, insbesondere der Logik und Mengenlehre. Die Teilnehmer sollten mit der Verwendung einer formalen Sprache vertraut sein und entsprechende Formeln verstehen.
Dauer	1

Lernziele

Nach Abschluss des Moduls verfügen die Studierenden über einen theoretisch fundierten und umfassenden Überblick über die Möglichkeiten der Spezifikation von Lösung und Problemen. Sie kennen ferner die Grundlagen der klassischen Spezifikations- und Lösungsmethoden. Außerdem verfügen sie über eine theoretisch fundierte Beurteilungsfähigkeit bezüglich der Grenzen von Berechenbarkeit und effizienter Lösbarkeit.

I.1.9.1 Berechenbarkeit und Komplexität

Lehrveranstaltung	Berechenbarkeit und Komplexität
Dozent(en)	Sebastian Iwanowski
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Vorlesung
Semesterwochenstunden	3
ECTS	2.5
Prüfungsform	Klausur / Mündliche Prüfung
Sprache	deutsch/englisch
Lehr- und Medienform(en)	Handout, Overheadfolien, Tafel

Lernziele

Nach Abschluss der Veranstaltung besitzen die Studierenden folgende Kompetenzen:

- Fundierter theoretischer Überblick über die Möglichkeiten des Problemlösens.
- Theoretisch fundierte Kenntnis der Grenzen der Berechenbarkeit und der effizienten Lösbarkeit.
- Kenntnis der Alternativen für die Praxis bei theoretisch unbefriedigenden Resultaten.

Inhalt

- Berechenbarkeit und Nichtberechenbarkeit
  - Präzisierung der Begriffe Problem und Algorithmen für die Theorie der Berechenbarkeit
  - Turingmaschinen im Detail
  - Komplexitätsklassen für Turingmaschinen
  - Beispiele für unentscheidbare Probleme
  - Beweise der Unentscheidbarkeit für ausgewählte Probleme
- NP-vollständige Probleme
  - Historie des P-NP-Problems
  - Beweis der NP-Vollständigkeit von SATISFIABILITY
  - Übersicht über NP-vollständige Probleme
  - Reduktionsmethode zum Beweis von NP-Vollständigkeit mit Beispielen
- Optimierungsaufgaben für NP-vollständige Probleme
  - Lösungstechniken für NP-vollständige Probleme
  - Übersicht über wichtige Anwendungen - Vergleich zu Verfahren der Künstlichen Intelligenz

Literatur

- Garey, Michael R.; Johnson, David S. (1979), Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman, ISBN 0-7167-1045-5
- Hopcroft, John E.; Motwani, Rajeev; Ullman, Jeffrey D.:
  Einführung in die Automatentheorie, Formale Sprachen und Komplexitätstheorie.
  2. überarb. Aufl. München: Addison-Wesley Longman Verlag, 2002.
- Vossen,Gottfried; Witt, Kurt-Ulrich:
  Theoretische Informatik.
  Braunschweig: Verlag Vieweg & Teubner 2004 (3. Auflage), ISBN 978-3528231477
- Wagenknecht, C.:
  Algorithmen und Komplexität,
  Fachbuchverlag Leipzig 2003
- Winter, R.:
  Theoretische Informatik,
  Oldenbourg-Verlag München 2002

I.1.9.2 Formale Spezifikation und Verifikation

Lehrveranstaltung	Formale Spezifikation und Verifikation
Dozent(en)	Ulrich Hoffmann
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Vorlesung mit integrierter Übung/Workshop/Assigm.
Semesterwochenstunden	3
ECTS	2.5
Prüfungsform	Klausur / Mündliche Prüfung
Sprache	deutsch/englisch
Lehr- und Medienform(en)	

Lernziele

Die Studierenden ...

- erlangen fundierte Kenntnisse der mathematischen Grundlagen der formalen Spezifikation und Verifikation.
- beherrschen verschiedene Spezifikationsstile.
- bekommen einen Einblick in verschiedene formale Spezifikationssprachen.
- erlangen die Fähigkeit, Spezifikationen systematisch zu konstruieren.
- können mathematische Beweise von Eigenschaften spezifizierte Software-Systeme führen.
- erlangen grundlegende Kenntnisse der Verifikation mit automatischen Beweissystemen.
- sind mit der Spezifikation von Sicherheitsbedingungen vertraut.
- können beurteilen, wie sich formale Methoden auf die IT-Sicherheit auswirken.

Inhalt

- Mathematische und logische Grundlagen der Spezifikation und Verifikation; Mengen, Multimengen, Verbände, partielle und totale Funktionen, algebraische Strukturen, Aussagen- und Prädikatenlogik, Modallogik, temporale Logik
- Algebraische Spezifikation; Terme, Gleichungen; Fallbeispiel einer algebraischen Spezifikation; Datenstrukturen, Operationen, Nachweis von Eigenschaften; maschinenunterstütztes Beweisen von Eigenschaften
- Modellorientierte Spezifikation; Fallbeispiel einer modellorientierten Spezifikation
- Konstruktion korrekter Programme aus Spezifikationen
- Aktuelle Spezifikationssprachen im Überblick

Literatur

- BJØRNER, Dines:
  Software Engineering 1.

Heidelberg: Springer Verlag, 2006

- DILLER, Antoni:
  Z An Introduction to Formal Methods.
  New York: Wiley & Sons, 1994
- EHRICH/GOGOLLA/LIPECK:
  Algebraische Spezifikation abstrakter Datentypen.
  Stuttgart: Teubner Verlag, 1989
- GOOS, Gerhard:
  Vorlesungen über Informatik Band 1 - Grundlagen und funktionales Programmieren.
  Heidelberg: Springer Verlag, 2005
- LAMPORT, Leslie:
  Specifying Systems.
  Amsterdam: Addison-Wesley, 2002
- SCHÖNING, Uwe:
  Logik für Informatiker.
  Heidelberg: Spektrum Akademischer Verlag, 2000
- WORDSWORTH, J., B.:
  Software Development with Z.
  New York: Addison-Wesley, 1992

I.1.10 Workshop Netzwerksicherheit

M121 Workshop Netzwerksicherheit

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M121
Bezeichnung	Workshop Netzwerksicherheit
Lehrveranstaltung(en)	M121a Workshop Netzwerksicherheit
Verantwortliche(r)	Dipl.-Ing. (FH) Ilja Kaleck
Zuordnung zum Curriculum	IT-Sicherheit (Master)
Verwendbarkeit	Das Modul ist sinnvoll mit den Inhalten des Moduls "Web- und Applikationssicherheit" zu kombinieren und ergänzt dessen Schwerpunkt im Bereich sicherheitsrelevanter Aspekte in der Softwareentwicklung mit notwendigen technischen Aspekten zum abgesicherten Aufbau und Betrieb IP-basierter Unternehmensnetze.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Die Studierenden benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium erworbene Fähigkeit zum analytischen Denken und zur Modellbildung. Weiterhin benötigen Sie die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium Kenntnisse der Funktionsweise eines modernen Computers bzw. Betriebssystems, sowie Kenntnisse über den Aufbau und Betrieb von IT- bzw. Rechnernetzen und der Programmierung.
Dauer	1

Lernziele

Die Studierenden lernen aktuelle technische Aspekte zum sicheren Aufbau und Betrieb IP-basierter Unternehmensnetze bzw. Computernetze in Hinblick auf ihre Sicherheit zu bewerten und bei dem Entwurf von Computernetzen grundlegende Sicherheitsaspekte zu beachten. Die Studierenden lernen die Prinzipien, nach denen Computernetzwerke in Teilnetze aufgeteilt werden und die technischen Methoden, mit denen so eine Aufteilung realisiert werden kann. Die Studierenden sind mit dem Entwurf und der Bewertung von Firewall-Regeln auf aktuellen Systemen vertraut. Sie können Techniken wie Intrusion Detection Systeme (IDS), den Einsatz von Proxy-Server Diensten sowie auch die Segmentierung des Netzes mit Hilfe der VLAN-Technik zielgerichtet zur Verbesserung der Netzwerksicherheit einsetzen. Sie wissen, wie sicherheits-

relevante Ereignisse detektiert und protokolliert werden und wie Protokolle in Hinblick auf Sicherheitsvorfälle ausgewertet werden müssen.

Zur Erreichung der Lernziele lösen die Studierenden praktische Aufgaben am eigenen Rechner unter Einbeziehung verschiedener Soft- und Hardwarekomponenten und komplexere Netzstrukturen bauen Sie unter Einsatz von Virtualisierungstechniken selbstständig nach. Sie präsentieren abschließend ihre Lösungen vor den anderen Teilnehmerinnen und Teilnehmern und dem Dozenten und fassen ihre Ergebnisse in einer kurzen schriftlichen Ausarbeitung zusammen.

I.1.10.1 Workshop Netzwerksicherheit

Lehrveranstaltung	Workshop Netzwerksicherheit
Dozent(en)	Ilja Kaleck
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Workshop
Semesterwochenstunden	4
ECTS	5.0
Prüfungsform	Abnahme
Sprache	deutsch
Lehr- und Medienform(en)	E-Learning, Handout, Online-Aufbereitung, Softwaredemonstration, studentische Arbeit am Rechner

Lernziele

Die Studierenden erlangen ...

- grundlegende Kenntnisse über den sicheren Aufbau und Betrieb moderner IP-basierter Unternehmensnetze
- die Fähigkeit, bestehende Netzwerke in Bezug auf ihre Sicherheitseigenschaft zu beurteilen und gezielt Schwachstellenanalyse zu betreiben
- aktuelle Werkzeuge zur Traffic-Analyse bzw. allgemeinen Network-Monitoring richtig einzusetzen und praktisch auch selbst nutzen zu können
- die Fähigkeit zum Aufbau sicherer VPN-Szenarien in Unternehmensnetze
- Kenntnisse über den praktischen Einsatz aktueller Verschlüsslungstechniken speziell in Computernetzwerken
- Kenntnisse über Zugriffskontrollmechanismen zu Netzwerken (logisch, physisch)
- Kenntnisse zur Herstellung von Ausfallsicherheit in typischen LAN-Strukturen

Inhalt

Grundlage der eigenständige Arbeit bildet der Aufbau einer eigenem virtualisierten Netzwerk- und Entwicklungsumgebung auf einem bzw. mehreren Workstations (PC) im Labor, darauf aufsetzend erfolgt

- die Konfiguration aktueller Netzkomponenten (Hardware) insbesondere in Bezug aus Sicherheitsaspekte
- eine elementare Cisco-Router bzw. Cisco IOS-Konfiguration, sowie Einsatz von Access Control Lists (ACL)zur Beschränkung des Datenflusses von Zugriffsrechten in Unternehmensnetzen
- eine grundlegende Firewall-Konfiguration (inkl. DMZ-Konzept, Einsatz von VLAN-Technik) und Entwicklung geeigneter Traffic-Management Konzepte (Traffic-Shaper, Proxy-Dienste)

- der Einsatz verschiedener VPN-Konzepte (IPsec, SSL-VPN) und ihre Konfiguration (Site-to-Site,
- der Einsatz von Zertifizierungsstellen zur Absicherung vertraulicher Übertragungskanäle
- der praktische Einsatz von LAN-Analyzer, IDS- und allg. Monitoring-Systemen in Netzen
- die Realisierung einer Layer-2 Anmeldesicherheit in LAN- und WLANs (u.a. per Radius-Server)
- die Einrichtung von allg. Layer-2 Sicherheit durch redundante Kopplung von Teilnetzen (Link-Aggregation Technik, Einsatz von Spanning-Tree Verfahren)

Literatur

- William Stallings: Cryptography and Network Security, Sixth Edition: Pearson, 2014
- Claudia Eckert: IT-Sicherheit, 9. Auflage 2014: Oldenbourg Verlag
- Günter Schäfer, Michael Roßberg: Netzsicherheit - Grundlagen und Protokolle, 2. Auflage 2014 ; dpunkt.Verlag
- Manfred Lipp: VPN - Virtuelle Private Netzwerke: Aufbau und Sicherheit, 1. Auflage, 2007: Addision-Wesley Verlag
- Eric F Crist, Jan Just Keijser: Mastering OpenVPN, 2015 : Packt Publishing
- John R., Vacca: Network and System Security, 2.ed, 2013: Syngress,
- Mike OLeary: Cyber Operations: Building, Defending, and Attacking Modern Computer Networks, 1.ed 2015: Apress
- James Baxter: Wireshark Essentials, 2014: Packt Publishing
- Justin Hutchens: Kali Linux Network Scanning Cookbook, 2014: Packt Publishing
- David Shaw: Nmap Essentials, 2015: Packt Publishing
- Matt Williamson: pfSense 2 Cookbook, 2011 : Packt Publishing
- Dirk van der Walt: FreeRadius - Beginners Guide, 2011: Packt Publishing
- Alexandre M.S.P. Moraes: Cisco Firewalls, 2011 : Cisco Press
- Christian Sperzel: Netzwerksicherheit, Video-Training 2014: video2brain.com
- Jörg Bueroße: Sichere E-Mails - Verschlüsselung und digitale Signatur, Videotraining 2014: video2brain.com
- Tom Wechsler: Einstieg in die Netzwerkanalyse mit Kali Linux, Videotraining 2015: video2brain.com
- Oliver Bauer, Michael Fritz: Wireshark Grundlagen, Videotraining 2015: video2brain.com

I.1.11 Distributed Systems

M035 Distributed Systems

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M035
Bezeichnung	Distributed Systems
Lehrveranstaltung(en)	M035a Distributed Systems M035b Tutorial: Distributed Systems
Verantwortliche(r)	Prof. Dr. Ulrich Hoffmann
Zuordnung zum Curriculum	IT Engineering (Master) IT-Sicherheit (Master) Informatik (Master) Wirtschaftsinformatik/IT-Management (Master)
Verwendbarkeit	Das Modul kann gut mit den Modulen "Funktionales Programmieren" und "Aktuelle Entwicklungen in der Informatik" sowie mit dem "Seminar-Master" kombiniert werden..
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Die praktischen Übungen setzen fortgeschrittene Programmierfähigkeiten voraus. Darüber hinaus setzt das Modul solide Kenntnisse der Internetarchitektur und -struktur sowie Grundkenntnisse der Ablauforganisation in Unternehmen voraus.
Dauer	1

Lernziele

Die Studierenden erwerben vertiefte Kenntnisse über technische Aspekte verteilter Systeme sowie deren Anwendungsgebiete in kommerziellen Kontexten. Sie erleben und diskutieren die technologischen inhärenten Probleme verteilter Systeme und sind dadurch in der Lage, sich den Herausforderungen verteilter Systeme, wie etwa Fragen der IT-Sicherheit oder der verschlüsselten Kommunikation, zu stellen und mit ihnen umzugehen. Sie kennen die Architektur und die wichtigsten Algorithmen in verteilten Systemen sowie die Prozesse in Entwicklung und Administration, die zu erfolgreichen verteilten Produkten führen. Sie sind in der Lage, verteilte Systeme in verschiedenen Programmierparadigmen zu programmieren.

I.1.11.1 Distributed Systems

Lehrveranstaltung	Distributed Systems
Dozent(en)	Ulrich Hoffmann
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Vorlesung
Semesterwochenstunden	2
ECTS	3.0
Prüfungsform	Klausur / Mündliche Prüfung
Sprache	english
Lehr- und Medienform(en)	

Lernziele

Die Studierenden gewinnen ...

- gründliches Verständnis der Prinzipien verteilter Anwendungen.
- Kenntnisse in der Beherrschung von Basistechnologien und aktuellen Software-Werkzeugen für verteilte Systeme.
- Zustandskenntnis der sind in verschiedenen Anwendungsbereichen wie Dienstleistungsvermittlung und E-Commerce.
- Kenntnisse über IT-Sicherheitsfragen in verteilten Systemen sowie über verschlüsselter Kommunikation.
- Kenntnisse der grundlegenden Algorithmen in verteilten Systemen.
- genaue Kenntnis der aktuellen Web-Service-Architekturen.
- praktische Fähigkeiten zur Realisierung eines Projekts.
- verteilte Programmierkenntnisse in verschiedenen Paradigmen.

Inhalt

- Praktische Beispiele
- Allgemeine Anforderungen an verteilte Systeme
- Die Client-Server-Beziehung und daraus resultierende Fragen
- Kommunikation in verteilten Systemen
- Dienste benennen
- Techniken für Gleichzeitigkeit
- Ferngespräche
- Alternative Paradigmen (Akteurskonzept, ...)
- Synchronisierung von Daten und Prozessen
- Koordinationsmethoden

- Replikationstechniken
- WEB-Dienste mit SOAP und REST
- Fehlertoleranzkonzepte
- Sicherheit in verteilten Systemen
- Programmierung mit Threads
- Kommunikation über Sockets, Struktur von Clients und Servern
- Ferner Prozeduraufruf / entfernter Methodenaufruf
- Verwendung von Benennungsdiensten
- Programmierung von WEB-Diensten (SOAP, Server/Client, WSDL, Datenbindung)
- verteiltes Programmieren mit alternativen Konzepten
- Programmierung von Synchronisierungsalgorithmen
- Programmierung verteilter Wahlalgorithmen
- Programmierung von REST-basierten Dienstleistungen und Kunden
- Fehlertolerante Programmierung in verteilten Systemen

Literatur

- ARMSTRONG, Joe:
  Programming Erlang.
  Pragmatic Programmers, 2007
- ODERSKY, Martin; SPOON, Lex; VENNERS, Bill:
  Programming in Scala.
  Artima Press, Mountain View, 2008
- COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim:
  Distributed Systems, Concepts and Design.
  Addison-Wesley, 2011, ISBN 0-1321-4301-1
- TANENBAUM, Andrew; VAN STEEN, Marten:
  Distributed Systems, Priciples and Paradigms.
  Prentice Hall, 2006, ISBN 0-1323-9227-5

I.1.11.2 Tutorial: Distributed Systems

Lehrveranstaltung	Tutorial: Distributed Systems
Dozent(en)	Ulrich Hoffmann
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Übung/Praktikum/Planspiel
Semesterwochenstunden	2
ECTS	2.0
Prüfungsform	Abnahme
Sprache	english
Lehr- und Medienform(en)	

Lernziele

Die Studenten ...

- erlangen die Fähigkeit, typische Softwaresysteme (Middleware) im Bereich der verteilten Systeme zu bedienen und zur Problemlösung einzusetzen.
- sind an Probleme gewöhnt, die in der Realität auftreten, und in der Lage, diese zu überwinden.
- haben einige praktische Erfahrungen mit IT-Sicherheitsfragen.
- wissen, wie man Verschlüsselung in verteilten Umgebungen einsetzt.
- eignen sich durch praktische Erfahrung ein tiefes Wissen über die spezifischen Eigenschaften verteilter Systeme an. Sie können diese Eigenschaften kategorisieren und bewerten.

Inhalt

Vorlesung mit begleitenden praktischen Übungen zur Programmierung verteilter Systeme und ihrer Algorithmen in verschiedenen Programmierparadigmen.

Literatur

- siehe Vorlesung
- Zahlreiche Online-Ressourcen

I.1.12 Projekt IT-Sicherheit

M047 Projekt IT-Sicherheit

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M047
Bezeichnung	Projekt IT-Sicherheit
Lehrveranstaltung(en)	M047a Projekt IT-Sicherheit
Verantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	IT-Sicherheit (Master)
Verwendbarkeit	Die Studierenden benötigen Kenntnisse der informatischen Grundlagen, um ein Projekt im Bereich der IT-Sicherheit erfolgreich durchzuführen. Die erworbenen Kenntnisse sind konkret auf Problemstellungen der IT-Sicherheit anwendbar. Darüber hinaus erwerben die Studierenden allgemeine Projektmanagement-Kompetenzen.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Die Studierenden benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium erworben Fähigkeit zum analytischen Denken und zur Modellbildung. Weiterhin benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium Kenntnisse der Funktionsweise eines modernen Computers und Betriebssystems, der Netzwerktechnik und der Programmierung.
Dauer	1

Lernziele

Nach Abschluss des Moduls verfügen die Studierenden über fortgeschrittene praktische Kenntnisse und Fähigkeiten in der IT-Sicherheit. Sie haben eine Sicherheitsanalyse eines praktisch genutzten IT-Produkts vorgenommen oder ein IT-System mit besonderen Anforderungen an die Sicherheit entwickelt.

Die Studierenden verfügen nach Abschluss des Moduls des Weiteren über soziale Kompetenzen im Bereich Projekt-Management. Die Studierenden sind in der Lage, sich auf die Projektdynamik und auf die kontinuierlichen Veränderungen während der Projektlaufzeit einzustellen. Sie sind in der Lage, Projekte auch im internationalen Kontext zu leiten.

I.1.12.1 Projekt IT-Sicherheit

Lehrveranstaltung	Projekt IT-Sicherheit
Dozent(en)	Gerd Beuster
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Projekt
Semesterwochenstunden	4
ECTS	5.0
Prüfungsform	Schriftl. Ausarbeitung (ggf. mit Präsentation)
Sprache	deutsch/englisch
Lehr- und Medienform(en)	interaktive Entwicklung und Diskussion von Modellen, Softwaredemonstration, studentische Arbeit am Rechner

Lernziele

Die Studierenden ...

- führen über weiterführende theoretische und praktische Kenntnisse in einem ausgewählten Bereich der IT-Sicherheit.
- verfügen über die Fähigkeit, in IT-Sicherheitsprojekten Leitungsfunktionen zu übernehmen.
- sind zur Arbeit in internationalen Teams befähigt.
- können die besonderen Anforderungen von IT-Sicherheitsprojekten im Change Management berücksichtigen.

Inhalt

Die Inhalte variieren von Veranstaltung zu Veranstaltung. Die Themensetzung orientiert sich an aktuellen Produkten und Entwicklungen in der IT-Sicherheit.

Literatur

Themenabhängig

I.1.13 Security Management

M049 Security Management

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M049
Bezeichnung	Security Management
Lehrveranstaltung(en)	M049a Security Management
Verantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	Betriebswirtschaftslehre (Master) IT Engineering (Master) IT-Management, -Consulting & -Auditing (Bachelor) IT-Sicherheit (Master) Wirtschaftsinformatik/IT-Management (Master) Wirtschaftsingenieurwesen (Master)
Verwendbarkeit	Das Modul setzt keine speziellen Kenntnisse voraus, allgemeine Fähigkeiten zum analytischen Denken und zur Modellbildung werden jedoch benötigt. Die im Modul erworbenen Kenntnisse können sowohl im Bereich des Security-Managements als auch in anderen Managementbereichen, insbesondere im Qualitäts-Management, verwendet werden.
Semesterwochenstunden	4
ECTS	5.0
Voraussetzungen	Die Studierenden benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium erworben Fähigkeit zum analytischen Denken und zur Modellbildung.
Dauer	1

Lernziele

In dem Modul Security Management lernen die Studierenden, IT-Sicherheit im Kontext von Unternehmensstrategien zu bewerten und zu gestalten. Die Studierenden lernen, Sicherheit als ganzheitliches Konzept zu erfassen, das nicht nur Software, sondern auch Hardware sowie administrative und physikalische Aspekte hat. Nach Abschluss des Moduls kennen sie die gesetzlichen und privatwirtschaftlichen Standards der Sicherheitsevaluierung und -zertifizierung. Sie können Sicherheitskonzepten und -richtlinien erstellen und praktisch umsetzen. Sie sind mit den gesetzlichen Grundlagen der IT-Sicherheit vertraut. Den Studierenden wird die Fähigkeit vermittelt, Management-Aufgaben im Bereich der IT-Sicherheit zu übernehmen und als IT-Sicherheitsmanager zu arbeiten. Sie sind in der Lage, in einem Unternehmen schützenswerte

Güter zu identifizieren und die zum Schutz notwendigen administrative Maßnahmen zu entwickeln und umzusetzen. Die Studierenden kennen die Schnittstellen zu und Überschneidungen mit anderen Bereichen des Managements, insbesondere des IT-Managements und des Change Managements.

I.1.13.1 Security Management

Lehrveranstaltung	Security Management
Dozent(en)	Gerd Beuster
Hörtermin	1
Häufigkeit	jährlich
Lehrform	Vorlesung mit integrierter Übung/Workshop/Assigm.
Semesterwochenstunden	4
ECTS	5.0
Prüfungsform	Klausur / Mündliche Prüfung
Sprache	english
Lehr- und Medienform(en)	E-Learning, interaktive Entwicklung und Diskussion von Modellen, Softwaredemonstration

Lernziele

In dem Modul Security Management lernen die Studierenden, IT-Sicherheit im Kontext von Unternehmensstrategien zu bewerten und zu gestalten. Den Studierenden wird die Fähigkeit vermittelt, Management-Aufgaben im Bereich der IT-Sicherheit zu übernehmen und als IT-Sicherheitsmanager zu arbeiten.

Sie erlangen die ...

- Fähigkeit, Bedrohungen zu identifizieren und zu modellieren.
- Fähigkeit, Risiken zu bewerten.
- Fähigkeit, die Angemessenheit von Sicherheitsmaßnahmen zu bewerten und angemessene Sicherheitsmaßnahmen zu konzipieren.
- Kenntnis der relevanten Standards und Zertifizierungsschemata im Bereich der IT-Sicherheit.
- Fähigkeit, IT-Sicherheit gesetzeskonform umzusetzen.
- Fähigkeit, IT-Sicherheit im Zusammenspiel mit organisatorischen und physischen Sicherheitsanforderungen und -maßnahmen zu gewährleisten.
- Kenntnisse der Zusammenhänge zwischen Sicherheits- und Qualitätsmanagement

Inhalt

- Einführung in das IT-Security-Management
- Unternehmenssicherheit als ökonomischer Faktor
- Angreifer und Angriffsziele
- Management sicherheitskritischer IT-Projekte
- IT-Grundschutz und ISO/IEC 27001
- Evaluierungs- und Zertifizierungsschemata in der IT-Sicherheit
- IT-Gesetzgebung

- Business Continuity Management
- Sicherheitstrainings
- Physikalische Sicherheit
- Sicherheitsaudits und Revisionskontrolle
- Sicherheitsmanagement und Qualitätsmanagement

Literatur

- BSI - Bundesamt für Sicherheit in der Informationstechnik: BSI-Standards 200-1, 200-2 und 200-3. Version 1.0. Bonn: BSI, 2017.
- Cole, Eric: Advanced Persistent Threat : Understanding the Danger and How to Protect Your Organization. Amsterdam, NL: Elsevier Syngress, 2012.
- Common Criteria for Information Technology Security Evaluation. Version 3.1 Revision 5. CCMB-2017-04-001. 2017.
- Gantz, Stephen D.: The Basics of IT Audit : Purposes, Processes, and Practical Information. Amsterdam, NL: Elsevier Syngress, 2014.
- Kersten, Heinrich; Klett, Gerhard: Der IT Security Manager. 3. Auflage. Wiesbaden: Springer Vieweg, 2013.
- Smith, Clifton L.; Brooks, David J.: Security Science : The Theory and Practice of Security. Oxford, UK: Butterworth-Heinemann, 2013.
- Snedaker, Susan: IT Security Project Management Handbook. Amsterdam, NL: Elsevier Syngress, 2006.
- Stallings, William: Computer Security : Principles and Practice. 4. Edition. London, UK: Pearson Education, 2017.
- Vacca, John R. (Hrsg.): Computer and Information Security Handbook. 3. Edition. Burlington (MA), USA: Morgan Kaufmann, 2017.
- Watson, David; Jones, Andrew: Digital Forensics Processing and Procedures. Amsterdam, NL: Elsevier Syngress, 2013.

I.1.14 Master-Thesis

M050 Master-Thesis

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M050
Bezeichnung	Master-Thesis
Lehrveranstaltung(en)	M050a Master-Thesis
Verantwortliche(r)	jeweiliger Dozent
Zuordnung zum Curriculum	Betriebswirtschaftslehre (Master) Data Science & Artificial Intelligence (Master) E-Commerce (Master) IT-Sicherheit (Master) Informatik (Master) Sustainable & Digital Business Management (Master) Wirtschaftsinformatik/IT-Management (Master) Wirtschaftsingenieurwesen (Master)
Verwendbarkeit	Keine
Semesterwochenstunden	0
ECTS	28.0
Voraussetzungen	Voraussetzung für die Master-Thesis ist der Stoff aus den vorangegangenen beiden Semestern, insbesondere der Veranstaltungen, die einen Bezug zur Themenstellung der Arbeit haben.
Dauer	1

Lernziele

In der Masterthesis zeigen die Studierenden, dass sie in der Lage sind, komplexe Aufgabenstellungen mit wissenschaftlich methodischer Vorgehensweise selbstständig und zielorientiert zu erarbeiten. Sie sind befähigt, Problemstellungen im größeren Kontext zu verorten, die fachlichen Zusammenhänge zu vernetzen und die gewonnenen Erkenntnisse argumentativ überzeugend darzustellen und zu präsentieren.

I.1.14.1 Master-Thesis

Lehrveranstaltung	Master-Thesis
Dozent(en)	jeweiliger Dozent
Hörtermin	3
Häufigkeit	jedes Semester
Lehrform	Thesis
Semesterwochenstunden	0
ECTS	28.0
Prüfungsform	Schriftl. Ausarbeitung (ggf. mit Präsentation)
Sprache	deutsch
Lehr- und Medienform(en)	Beamerpräsentation, Tafel

Lernziele

Die Studierenden sind in der Lage ...

- komplexe Aufgabenstellungen selbständig zu erarbeiten.
- Problemstellungen im größeren Kontext zu verorten.
- wissenschaftliche Methoden für die Problemlösung einzusetzen.
- Ergebnisse überzeugend darzustellen.

Inhalt

themenabhängig

Literatur

themenabhängig

I.1.15 Master-Kolloquium

M058 Master-Kolloquium

Studiengang	Master-Studiengang IT-Sicherheit
Kürzel	M058
Bezeichnung	Master-Kolloquium
Lehrveranstaltung(en)	M058a Kolloquium
Verantwortliche(r)	jeweiliger Dozent
Zuordnung zum Curriculum	Betriebswirtschaftslehre (Master) Data Science & Artificial Intelligence (Master) E-Commerce (Master) IT-Sicherheit (Master) Informatik (Master) Sustainable & Digital Business Management (Master) Wirtschaftsinformatik/IT-Management (Master) Wirtschaftsingenieurwesen (Master)
Verwendbarkeit	Keine
Semesterwochenstunden	0
ECTS	2.0
Voraussetzungen	Zulassungsvoraussetzung zum Kolloquium ist eine mit mindestens "ausreichend" bewertete Master-Thesis.
Dauer	1

Lernziele

Die Studierenden präsentieren ihre Arbeitsergebnisse überzeugend vor dem Prüfungsausschuss. Sie beherrschen das Instrument der freien Rede, argumentieren schlüssig und beweisführend. In einer anschließenden fächerübergreifenden mündlichen Prüfung verteidigen sie ihre Arbeitsergebnisse und erweisen sich in der Diskussion als problemvertraut.

I.1.15.1 Kolloquium

Lehrveranstaltung	Kolloquium
Dozent(en)	verschiedene Dozenten
Hörtermin	3
Häufigkeit	jedes Semester
Lehrform	Kolloquium
Semesterwochenstunden	0
ECTS	2.0
Prüfungsform	Kolloquium
Sprache	deutsch
Lehr- und Medienform(en)	

Lernziele

Die Studierenden ...

- besitzen die Fähigkeit der konzentrierten Darstellung eines intensiv bearbeiteten Fachthemas.
- verfestigen die Kompetenz, eine fachliche Diskussion über eine Problemlösung und deren Qualität zu führen.
- verfügen über ausgeprägte Kommunikations- und Präsentationsfähigkeiten.

Inhalt

- Fachvortrag über Thema der Master-Thesis sowie über die gewählte Vorgehensweise und die Ergebnisse
- Diskussion der Qualität der gewählten Lösung
- Fragen und Diskussion zum Thema der Master-Arbeit und verwandten Gebieten

Literatur

themenabhängig

Dokumenttyp	Modulhandbuch
Abschlusstyp	Master
Studiengangname	IT-Sicherheit
Ordnungsnummer	19.0
Setzdatum	16. Dezember 2021
git	ja
git-commit	99b702a1 (lokale Änderungen vorhanden)