Technische Hochschule Ingolstadt

Modulhandbuch

Cloud Applications und Security Engineering (SPO WS 22/23)

Master

Fakultät für Informatik

Stand: 08.08.2022

Inhalt

1 Zusammenfassung

Dieses Dokument beschreibt das aktuelle Lehrangebot im Masterstudiengang Cloud Applications und Security Engineering.

Insbesondere legt es die Studienziele und Studieninhalte der einzelnen Pflichtmodule, der fachwissenschaftlichen Wahlpflichtmodule, sowie die zeitliche Aufteilung der Semesterwochenstunden je Modul und Studiensemester dar.

Es enthält weiterhin die näheren Bestimmungen über studienbegleitende Leistungs- und Teilnahmenachweise.

Bei Mehrdeutigkeiten hat die übergeordnete Studien- und Prüfungsordnung Vorrang.

2 Einführung und Studienaufbau

2.1 Studienziel und Kompetenzprofil

Ziel des weiterqualifizierenden Masterstudiengangs Cloud Applications und Security Engineering ist die Vermittlung informatikbezogenen Wissens. Auf der Grundlage wissenschaftlicher Erkenntnisse und Methoden werden Hochschulabsolventen auf Führungs- und Expertenaufgaben in Unternehmen und Organisationen vorbereitet. Der Studiengang vermittelt neben fachlichem und methodischem Wissen auch Anstöße zur Entwicklung sozialer Kompetenzen. Ebenso fördert er das selbständige wissenschaftliche Arbeiten mit Fokus auf der angewandten Forschung.

Der Masterstudiengang Cloud Applications und Security Engineering baut inhaltlich auf dem grundständigen Bachelorstudiengang Informatik der Technischen Hochschule Ingolstadt auf und vertieft fachwissenschaftliche Kenntnisse und Kompetenzen in den Themengebieten der Softwaretechnik für Enterprise Applications und verteilter Datenhaltung und -verarbeitung sowie Entwicklung, Betrieb und Bereitstellung von Anwendungen in Cloud-Infrastrukturen wie auch Methoden und Strategien für die Entwicklung und den Betrieb von sicheren IT-Infrastrukturen und -Anwendungen.
Darüber hinaus werden die analytische Kompetenz und Methodenkompetenz der Studierenden weiter gestärkt, ebenso wie ihre Fähigkeit zur Reflexion des eigenen Handelns und Verhaltens.

Der Master qualifiziert wahlweise für eine Position als Fachexperte, Projektleiter oder als Führungskraft in Unternehmen, im höheren Dienst öffentlicher Einrichtungen oder für eine Tätigkeit im wissenschaftlichen Bereich (dies schließt die Möglichkeit der Promotion ein).

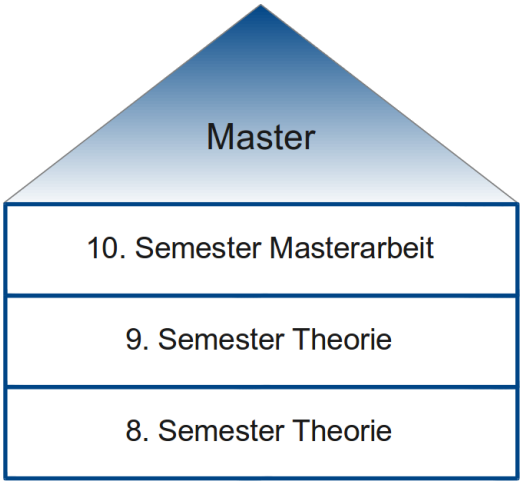
2.2 Studienabschluss

Die Technische Hochschule Ingolstadt verleiht nach erfolgreicher Abschlussprüfung den folgenden akademischen Grad:

Master of Science (M.Sc.)

2.3 Studienaufbau

Das Studium wird als Vollzeitstudium angeboten. Die Regelstudienzeit beträgt drei Studiensemester (90 ECTS-Punkte), wobei das dritte Semester überwiegend der Anfertigung der Masterarbeit dienen soll.



2.4 Qualifikationsvoraussetzungen

Qualifikationsvoraussetzungen für den Zugang zum Masterstudiengang sind[1]:

a) Der Nachweis eines erfolgreichen Abschlusses eines Studiums im Bereich Informatik oder einem artverwandten Bereich an einer deutschen Hochschule mit mindestens 210 ECTS-Leistungspunkten oder äquivalentem Studienumfang oder ein gleichwertiger erfolgreicher in- oder ausländischer Abschluss.

b) Dringend empfohlen werden Grundkenntnisse in den Bereichen Mathematik, Betriebssystemen, Rechnernetze, Da- tenbanksysteme / Datenmanagement, Programmiersprachen, Softwareengineering und IT-Sicherheit, wie sie beispielsweise in einem Studium nach a) enthalten sind.

Hinsichtlich der zeitlichen Rahmenbedingungen für die Erbringung des Nachweises wird auf die Studien- und Prüfungsordnung (SPO) Cloud Applications und Security Engineering, §3 (3) verwiesen. Hinsichtlich der Zulassung von Bewerbern, die ein abgeschlossenes Hochschulstudium bzw. einen gleichwertigen Abschluss nachweisen, für das weniger als 210, jedoch mindestens 180 ECTS-Punkte vergeben wurden, wird auf die SPO Cloud Applications und Security Engineering, §3 (4) verwiesen.

Näheres regelt die SPO Cloud Applications und Security Engineering.

[1] rechtlich verbindlich für Vorrückungs- und Zulassungsvoraussetzungen ist nur die SPO Cloud Applications und Security Engineering

2.5 Studiengangleitung

Für Fragen die organisatorische Abwicklung des Studiengangs betreffend, steht der Studiengangleiter zur Verfügung:

Prof. Dr. Sebastian Apel, Gebäude A, Raum A 128, Tel. 0841 / 9348 – 5176

Die während des Semesters geltenden Sprechstunden werden jeweils durch Aushang bzw. über die e-Learning-Plattform Moodle der THI bekannt gemacht.

2.6 Fachstudienberatung

Für alle fachlichen Fragen und Probleme im Zusammenhang mit dem Studium steht der Fachstudienberater zur Verfügung:

Prof. Dr. Sebastian Apel, Gebäude A, Raum A 128, Tel. 0841 / 9348 – 5176

Die während des Semesters geltenden Sprechstunden werden jeweils durch Aushang bzw. über die e-Learning-Plattform Moodle der THI bekannt gemacht.

3 Curriculare Struktur

Der Masterstudiengang Cloud Applications und Security Engineering beginnt jedes Sommer- und jedes Wintersemester. In der Regel werden die einzelnen Module entweder im Sommersemester oder im Wintersemester angeboten.

Die Inhalte der Module des Sommersemesters sind unabhängig von den Inhalten der Module des Wintersemesters und umgekehrt. Dadurch ist gewährleistet, dass der Einstieg in das Masterstudium sowohl im Winter als auch im Sommer möglich ist.

Die Studierenden des ersten und zweiten Semesters nehmen in der Regel gemeinsam an den Veranstaltungen teil. Die folgende Tabelle stellt das Curriculum dieser Semester dar, wobei die Module der ersten beiden Semester aus oben genannten Gründen nach Sommer- und Wintersemester gruppiert sind und nicht nach erstem und zweitem Semester.

Das dritte Semester ist für die Anfertigung der Masterarbeit (30 CP) vorgesehen.

3.1 Module der ersten beiden Semester

Lfd. Nr.	Modul	Sommersemester		Wintersemester	
		SWS	CP	SWS	CP
1	Architektur- und Entwurfsmuster der Softwaretechnik	4	5 (schrP)		
2	Cloud-native Development			4	5 (prA)
3	Security Engineering in der IT	4	5 (schrP)		
4	Computer-Forensik und Vorfallsbehandlung	4	5 (prA)		
5	Ereignisbasierte Dateninfrastrukturen	4	5 (schrP)		
6	Sicherheit moderner Netzwerke			4	5 (schrP)
7	Fachwissenschaftliches Wahlpflichtmodul 1			4	5 (LN)
8	Fachwissenschaftliches Wahlpflichtmodul 2			4	5 (LN)
9	Fachwissenschaftliches Wahlpflichtmodul 3	4	5 (LN)		
10	Interdisziplinäres fachwiss. Wahlpflichtmodul	4	5 (LN)		
11	Seminar			2	3 (SA)
12	Projekt			4	7 (PA)
	Summe	**24**	**30**	**22**	**30**

Legende:

LN	Leistungsnachweis
mdlP	mündliche Prüfung
PA	Projektarbeit
prA	praktische Arbeit
SA	Seminararbeit
schrP	schriftliche Prüfung

Näheres zu den o.a. Prüfungsformen regelt die SPO Cloud Applications und Security Engineering.

3.2 Fachwissenschaftliche Wahlpflichtmodule

Als fachwissenschaftliche Wahlpflichtmodule werden die (Plicht-)Module des Masterstudiengangs Business Information Systemen Engineering, sowie ggfs. weitere angeboten.

Nähere Informationen zu diesen Modulen, sowie ihre Zuordnung zu Sommer- bzw. Wintersemester (und damit auch das resultierende Semesterangebot dieser Module als fachwissenschaftliche Wahlpflichtmodule im Masterstudiengang Cloud Applications und Security Engineering), sind im Modulhandbuch des Masterstudiengangs Business Information Systems Engineering aufgeführt.

4 Besonderer Hinweis

Wichtig:

Ist zur Ablegung einer Wiederholungsprüfung die **aktive Teilnahme an einer nicht angebotenen Lehrveranstaltung notwendig**, z.B. bei Praktika und Seminaren, so ist der Studierende verpflichtet, dies in den **ersten drei Semesterwochen mit dem zuständigen Studiengangleiter zu besprechen**.

Nach Ablauf dieser Frist besteht für den Studierenden kein Anspruch mehr darauf, diese Wiederholungsprüfung im aktuellen Semester ablegen zu können!

5 Modulbeschreibungen

5.1 Allgemeine Pflichtmodule

Architektur- und Entwurfsmuster der Softwaretechnik			
Modulkürzel:	CASE_AES	**SPO-Nr.:**	1
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hafenrichter, Bernd
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Architektur- und Entwurfsmuster der Softwaretechnik
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Prüfungsleistungen:	schrP90 - schriftliche Prüfung, 90 Minuten
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Grundlegende Erfahrung in der Entwicklung kleinerer Software-Systeme und damit verwandter Technologien (UML, Programmierung, Datenbanken)

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls sind die Studierenden in der Lage,

- die Bedeutung der Software-Architektur und deren Einfluss auf den Lebenszyklus einer Software wiederzugeben
- Funktionale und Nicht-Funktionale-Anforderung auf verschiedene Ebenen einer Architektur abzubilden
- komplexe Software-Architekturen zu entwerfen und umzusetzen
- das Prinzip Inversion of Control auf Basis einer objektorientierten Programmiersprache anzuwenden
- Anforderung auf ein wohl strukturiertes Software-Design zu übertragen
- einen Katalog an Design-Patterns zu beschreiben und können diese auf konkrete Problemstellungen übertragen.
- die Vor- und Nachteile der verschiedenen Muster und die Auswirkung auf das Design einzuschätzen
- die wichtigsten Bestandteile professioneller Buildumgebungen aufzuzählen

Inhalt:

1. Grundlagen:
   - Definition Software Architektur
   - Grundprinzipien
2. Struktursicht
   - Komponentenarchitektur
   - Aufbau eines Komponentenframeworks mit Inversion of Control und Dependency Injection
   - Quasar
   - Diskussion anhand eines Beispiels
3. Physische Sicht
   - Verteilungsmuster
   - Verfügbarkeit von verschiedenen Verteilungsmuster
   - Clustering
4. Process Sicht
   - Grundlegend Muster
   - Muster für Auftragsverarbeitende Server
   - Diskussion anhand eines Beispiels
   - Asynchrone Programmierung
5. Die logische Sicht
   - Designprinzipien
   - Domain Driven Design
     - Grundlagen
     - Supple Design
     - Maintaining the Modell Integrity
6. Microservice Architecture
   - Patterns für Microservices
7. Design Pattern
   - Erzeugerpattern
   - Strukturpattern
   - Verhaltenspattern
8. Enterprise Patterns
   - Logical Unit Of Work
9. Entwicklungsumgebung
   - Buildserver
   - Testumgebung
   - Continuos Integration und Delivery

Literatur:

- GOLL, Joachim, 2014. *Architektur- und Entwurfsmuster der Softwaretechnik: mit lauffähigen Beispielen in Java* [online]. Wiesbaden: Springer Fachmedien PDF e-Book. ISBN 978-3-658-05531-8, 978-3-658-05532-5. Verfügbar unter: https://doi.org/10.1007/978-3-658-05532-5.
- SIEDERSLEBEN, Johannes, 2006. *Moderne Softwarearchitektur: umsichtig planen, robust bauen mit Quasar*. 1. Auflage. Heidelberg: dpunkt-Verl.. ISBN 3-89864-292-5
- MARTIN, Robert C., . *Clean Code: A Handbook of Agile Software Craftsmanship*.
- FOLWER, Martin, . *Patterns of Enterprise Application Architecture*.
- EVANS, Eric J., . *Domain-Driven Design: Tackling Complexity in the Heart of Software*.

Anmerkungen:
Keine Anmerkungen

Cloud-native Development

Modulkürzel:	CASE_CND	**SPO-Nr.:**	2
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Apel, Sebastian
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 79 h Gesamtaufwand: 126 h
Lehrveranstaltungen des Moduls:	Cloud-native Development
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Prüfungsleistungen:	prA - Praktische Arbeit inkl. Abnahmegespräch von 30 min.
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Aus dem bereits absolvierten Bachelor-Studiengang sollten folgende Grundlagen vorhanden sein: Relationale Datenbanksysteme, Netzwerktechnik (TCP/IP) Stack, Client/Server-Modell, Programmiersprachen (Java, Python), Revision Control (Mercurial oder Git), Statistik (Lineare Regressionsrechnung, Verteilungen, Hypothesentests), Grundkenntnisse in Linux (Installation und Konfiguration von Programmen, Arbeiten auf der Kommandozeile).

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- kennen die Studierenden aktuelle Technologien, die die Basis bilden für skalierbare Anwendungen im Web- und Cloud-Kontext
- kennen die Studierenden Referenzarchitekturen und Architekturstile in verteilten (webbasierten) Anwendungen in der Cloud und damit notwendige Dienste zur Orchestrierung der Systemlandschaft
- kennen die Studierenden den Unterschied zwischen Virtualisierung und Containerisierung
- können die Studierenden eine einfache virtualisierte Instanz aufzusetzen
- können die Studierenden eine (webbasierte) Anwendung über ein Containerformat bereitstellen
- können die Studierenden eine einfache skalierbare verteilte Anwendung in Java umsetzen und in einer Cloud-Infrastruktur zur Aufführung bringen

Inhalt:

- Grundbegriffe im Kontext webbasierter skalierbarer Anwendungen
- Rückblick: Relationale Datenbanksysteme, webbasierte Systeme, Client/Server-Modell, Revision Control und Kommandozeilen

- Virtualisierung vs. Containerisierung - Theoretische Einführung und praktische Erprobung
- Architekturstile und Referenzarchitekturen für verteilte Anwendungen
- Orchestrierungssysteme
- Infrastruktur für verteilte (webbasierte) Anwendungen (Konfiguration, Netzwerke, Gateways und Dienst-Lokalisierung)
- Beispielhafte Umsetzung einer skalierbaren (webbasierte) Anwendung

Literatur:

- HÜTTERMANN, Michael, 2012. *DevOps for Developers* [online]. Berkeley, CA: Apress PDF E-Book. Verfügbar unter: https://doi.org/10.1007/978-1-4302-4570-4.
- NADAREISHVILI, Irakli und andere, July 2016. *Microservice architecture: aligning principles, practices, and culture*. F. Auflage. Beijing; Boston ; Farnham ; Sebastopol ; Tokyo: O'Reilly. ISBN 978-1-491-95625-0
- WOLFF, Eberhard, 2018. *Microservices: Grundlagen flexibler Softwarearchitekturen*. 2. Auflage. Heidelberg: dpunkt.verlag. ISBN 978-396088-413-2, 978-3-96088-414-9
- ARUNDEL, John und Justin DOMINGUS, February 2019. *Cloud native devops with Kubernetes: building, deploying and scaling modern applications in the cloud*. F. Auflage. Beijing, Boston, Farnham, Sebastopol, Tokyo: O'Reilly. ISBN 978-1-4920-4076-7

Anmerkungen:

Jeder Teilnehmer realisiert im Kontext des Cloud-native Developments eine Beispielanwendung bestehend aus mindestens zwei Diensten, welche in der Cloud betrieben werden, kann. Am Ende des Semesters werden Vorgehensweise und Ergebnisse bei der Durchführung der praktischen Arbeit in einer Kurzpräsentation erläutert und eine Dokumentation der praktischen Arbeit beim Dozenten abgegeben.

Security Engineering in der IT

Modulkürzel:	CASE_SEIT	**SPO-Nr.:**	3
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hof, Hans-Joachim
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Security Engineering in der IT
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Prüfungsleistungen:	schrP90 - schriftliche Prüfung, 90 Minuten
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Vertiefte Kenntnisse in den Bereichen Betriebssysteme, Netzwerke, Programmierung, Softwareengineering sowie Grundkenntnisse IT-Sicherheit

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- verfügen die Studenten über grundlegende Kenntnisse zu Designprinzipien sicherer IT-Systeme, insbesondere unter Berücksichtigung moderner verteilter Systeme.
- entwickeln Studenten einerseits ein Verständnis dafür, wie sich Systeme unter Einsatz moderner Virtualisierungstechniken, spezieller Hardware sowie geeigneten Maßnahmen bei Einsatz moderner Betriebssysteme härten lassen.
- erlangen die Studenten durch die Veranstaltung andererseits vertiefte Kenntnisse darüber, welche Techniken des Softwareengineering im besonderen Maße auf die Sicherheit aktueller Software abzielen und wie sicherheitsrelevante Schnittstellenrisiken vermieden werden.

Inhalt:

- Sichere Softwareentwicklung (Benutzereingaben, Privilegien, Protokolle)
- Absicherung von Kommunikationswegen und Schnittstellen
- Verschlüsselung, Algoritmen zum Schlüsselaustausch, Einsatz von Zertifikaten
- Systemhärtung auf Betriebesystemebene
- Datensicherheit (Privilegien Filesystem, ACLs)
- Sicherheit bei Multi-Thier-Systemen
- Absicherung von Datenbanken und Webfrontends

- Virtualisierungstechniken, Sandbox
- Updatestrategien
- interne Sicherheits-Audits, Pentests und Security Patching
- Sicherheitsfunktionen moderner Software
- Code Obfuscation
- Techniken zur Authentifizierung und Identifizierung
- Backupstrategien unter Sicherheitsgesichtspunkten, sichere Datenaufbewahrung

Literatur:

- ANDERSON, Ross, 2020. *Security engineering: a guide to building dependable distributed systems*. T. Auflage. Indianapolis: Wiley. ISBN 1-119-64278-7, 978-1-119-64278-7
- MEAD, Nancy R. und Carol C. WOODY, 2017. *Cyber security engineering: a practical approach for systems and software assurance*. Boston: Addison-Wesley. ISBN 978-0-134-18980-2, 0-134-18980-9
- PAULUS, Sachar, 2011. *Basiswissen sichere Software: Aus- und Weiterbildung zum ISSECO Certified Professional for Secure Software Engineering*. 1. Auflage. Heidelberg: Dpunkt.verlag. ISBN 978-3-89864-726-7, 978-3-86491-052-4

Anmerkungen:

Keine Anmerkungen

Computer-Forensik und Vorfallsbehandlung

Modulkürzel:	CASE_CFV	SPO-Nr.:	4
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Hahndel, Stefan
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Computer-Forensik und Vorfallsbehandlung
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Prüfungsleistungen:	prA - Praktische Arbeit inkl. Abnahmegespräch von 30 min.
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Grundlagen der Programmierung/Programmierkenntnisse; Grundkenntnisse Betriebssysteme; Grundkenntnisse IT-Sicherheit

Angestrebte Lernergebnisse:

Nach erfolgreicher Absolvierung des Moduls sind die Studierenden in der Lage,

- theoretische Grundlagen der Computer-Forensik und entsprechende Prozessmodelle basierend auf Carrier's Hypothesen-basierten Ansatz und seinem Referenzmodell für Daten auf Dateisystemen wiederzugeben.
- wichtige Angriffsmuster auf Computersysteme zu beschreiben und wissen, welche Spuren diese hinterlassen.
- Dateisysteme einer forensischen Analyse zu unterziehen.
- die wichtigsten Methoden zu Netzwerk-/Internet-Forensik und Malware Analyse zu beschreiben.

Inhalt:

- Methoden von Angreifern und typische Angriffsmuster
- Prozessmodelle für Forensic Computing
- Technologie moderner Speichersysteme: Harddisk, SSDs, DRam, Flash, MRams etc.
- Disk Volumes und Partitionen im Detail
- Diverse Dateisysteme, Verfahren zur Wiederherstellung von Daten (FAT, NTFS und Unix/Linux-Dateisysteme)
- Netzwerk und Internet-Forensik: z.B. Aufspüren von HTTP-Requests und Emails

- Fortgeschrittene Werkzeuge zur Computer-Forensik
- Umgang mit verschlüsselten Daten, Aufspüren von Verschlüsselung
- Grundlagen der Multimedia-Forensik (Analyse von Bild- und Audiodaten)
- Fortgeschrittene Carvingtechniken

Literatur:

- GESCHONNECK, Alexander, 2014. *Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären*. 6. Auflage. Heidelberg: dpunkt.verlag. ISBN 978-3-86491-489-8, 978-3-86491-490-4
- KUHLEE, Lorenz und Victor VÖLZOW, 2012. *Computer-Forensik Hacks*. 1. Auflage. Beijing [u.a.]: O'Reilly. ISBN 978-3-86899-121-5, 3-86899-121-2
- WILLER, Christoph, 2012. *PC-Forensik: [Daten suchen und wiederherstellen]*. 1. Auflage. Böblingen: C & L, Computer- und Literaturverl.. ISBN 978-3-936546-60-6, 3-936546-60-6
- DEWALD, Andreas und Felix C. FREILING, 2015. *Forensische Informatik*. 2. Auflage. Norderstedt: BoD - Books on Demand. ISBN 978-3-842-37947-3
- CARRIER, Brian, 2005. *File system forensic analysis*. Upper Saddle River, NJ: Addison-Wesley. ISBN 0-321-26817-2, 978-0-32-126817-4
- SIKORSKI, Michael und Andrew HONIG, 2012. *Practical malware analysis: the hands-on guide to dissecting malicious software*. San Francisco: No Starch Press. ISBN 978-1-59327-290-6, 1-59327-290-1
- LIGH, Michael Hale und andere, 2014. *The art of memory forensics: detecting malware and threats in Windows, Linux, and Mac memory*. Somerset: Wiley. ISBN 978-1-118-82504-4, 978-1-118-82499-3

Anmerkungen:

Jeder Teilnehmer bekommt eine konkrete praktische Fragestellung aus dem Bereich der Computerforensik zur individuellen Bearbeitung während des Semesters. Am Ende des Semesters werden Vorgehensweise und Ergebnisse bei der Durchführung der praktischen Arbeit in einer Kurzpräsentation erläutert und eine Dokumentation der praktischen Arbeit beim Dozenten abgegeben.

Ereignisbasierte Dateninfrastrukturen

Modulkürzel:	CASE_EDI	**SPO-Nr.:**	5
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	1
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Sommersemester

Modulverantwortliche(r):	Apel, Sebastian
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 79 h Gesamtaufwand: 126 h
Lehrveranstaltungen des Moduls:	Ereignisbasierte Dateninfrastrukturen
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Prüfungsleistungen:	schrP90 - schriftliche Prüfung, 90 Minuten
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Aus dem bereits absolvierten Bachelor-Studiengang sollten folgende Grundlagen vorhanden sein: Relationale Datenbanksysteme, Netzwerktechnik (TCP/IP) Stack, Client/Server-Modell, Programmiersprachen (Java, Python), Revision Control (Mercurial oder Git), Statistik (Lineare Regressionsrechnung, Verteilungen, Hypothesentests), Grundkenntnisse in Linux (Installation und Konfiguration von Programmen, Arbeiten auf der Kommandozeile).

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- kennen die Studierenden grundlegende Technologien, die die Basis bilden für Datenhaltungs- und Analysesysteme, welche Datenströme speichern und bearbeiten können
- verstehen die Studierenden, dass große Datenmengen mit ausschließlich vertikal skalierenden Systemen nicht beherrscht werden können, und horizontal skalierbare ereignisbasierte Ansätze erfolgversprechend sind
- kennen die Studierenden unterschiedliche Ausprägungen des verteilten Verarbeitens von Datenströmen, kennen deren wesentliche Eigenschaften und können die Stärken- und Schwächen der einzelnen Varianten im Kontext ereignisbasierter Ansätze benennen
- können die Studierenden Strategien zum Austausch von Nachrichten und Ereignissen in stark verteilten Systemen, insbesondere Cloud-Umgebungen, anwenden
- können die Studierenden asynchrone Ansätze zur Verarbeitung von Nachrichten und Ereignissen umsetzen
- sind die Studierenden in der Lage, abhängig von der Problemstellung, eine geeignete Ausprägung des verteilten Rechnens und der verteilten Datenhaltung auszuwählen

Inhalt:
1. Grundlagen im Kontext von Events, Messaging, Big Data, IoT und Parallelisierung 2. Asynchroner Austausch von Nachrichten in stark verteilten Systemen 3. Ereignisgetriebene Programmierkansätze 4. Ereignisbasierte Abfragesprachen 5. Skallierbare Infrastruktur zur Analyse von Nachrichten 6. Complex Event Processing 7. Konzepte und Implementierung der verteilten Datenhaltung
Literatur:
Wird zu Beginn bekannt gegeben
Anmerkungen:
Keine Anmerkungen

Sicherheit moderner Netzwerke

Modulkürzel:	CASE_SMN	**SPO-Nr.:**	6
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Jarschel, Michael
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 47 h Selbststudium: 78 h Gesamtaufwand: 125 h
Lehrveranstaltungen des Moduls:	Sicherheit moderner Netzwerke
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Prüfungsleistungen:	schrP90 - schriftliche Prüfung, 90 Minuten
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Besuch der Vorlesung und des Praktikums Rechnernetze (Voraussetzung), empfehlenswert ist der Besuch des FW-Fachs "Internet - Netz der Netze"

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an der Lehrveranstaltung sind die Studierenden in der Lage,

- typische Angriffsszenarien auf Rechnernetze aufzuzählen und zu erklären;
- Schutzmaßnahmen, insbesondere passende Protokolle, auszuwählen und zu beurteilen;
- die prinzipielle Struktur des Internets, das Architekturmodell der Kommunikation (TCP/IP-Schichtenmodell) im Detail, TCP-Protokoll-Eigenschaften und -Verhalten im Prinzip sowie auch die Grundlagen der Vermittlungstechniken zu beschreiben;
- Performance und Wartezeiten der Paketvermittlung abzuschätzen;
- die Architektur eines Routers darzustellen und typische Maßnahmen zur Erhöhung der Ausfall-Sicherheit in IP-Netze zu kennen;
- die generelle Struktur der heutigen öffentlichen IP-Netze mit allen Technologie-Schichten und deren prinzipiellen Funktionen, Netzelementen und Sicherheitsaspekten zu benennen;
- die Entwicklung, Architektur und Funktion der aktuellen Funknetzwerke, insbesondere der Mobilfunk-Generationen für Sprache und Daten, mit speziellem Blick auf die relevanten Sicherheitsfunktionen wiederzugeben

Inhalt:

1. Grundlagen des Internets und der Paketvermittlung:
   - Architekturmodell, Dienste-und Schichtenkonzept

- Grundlagen der Paketvermittlung und der Performance
- Vertiefung des Transportprotokolls TCP: Flusskontrolle und Überlastkontrolle
- Typische Angriffe im Internet

2. Netzwerk-Sicherheit:
   - Typische Attacken und Schutzmaßnahmen vor Angreifern
   - Operative Sicherheit / Netzwerk-Sicherheitsarchitektur (u.a. Firewalls, Gateways, IDS)
   - Protokolle zur sicheren Kommunikation (u.a. TLS, IPSec, Signal, SSH)
3. Funknetze
   - Bluetooth
   - WLAN/Wi-Fi/802.11
   - Mobilfunk-Haupteigenschaften
   - A-/B-/C-Netze (1G): Historische Entwicklung der Mobilfunknetze
   - GSM (2G, D-/E-Netze):
     - Luftschnittstelle, Sprachkodierung, Netzarchitektur
     - Identitäten (SIM-Karte) und Verschlüsselung, Authentisierung, Angriffsvektoren
     - Erweiterung für Daten: GPRS/EDGE
   - UMTS (3G):
     - Luftschnittstelle mit WCDMA
     - Sicherheitsarchitektur
     - Erweiterung für Daten: HSPA
   - LTE/LTE+ (4G):
     - Luftschnittstelle, Übertragungstechnik
     - Sicherheitsarchitektur
     - Netzstruktur (evolved Packet Core)
   - 5G
     - Evolution LTE zu 5G
     - Ziele und Ansätze von 5G, Anwendungen
     - Einführungsszenarien, Migration der Netze
4. Struktur des Internets (Festnetz):
   - Anforderungen an den sicheren Betrieb eines Kommunikationsnetzes
   - Netzzugang (Access): Technologien und typische Übertragungsmedien (DSL, Fttx, HFC, PON)
   - Elemente und Funktionen des optischen Transportnetzes (WDM-Netz)
   - Elemente und Funktionen des synchronen TDM-Transportnetzes (SDH) inkl. Funktionen zur Ersatzschaltung
   - Struktur aktueller Router und Maßnahmen für den sicheren Betrieb
   - Struktur des IP-Backbones (nationales Netz) und Beispiele für die aktuellen Entwicklungen der Netze (u.a. Virtualisierung, SDN, neue Netzkonzepte)

Literatur:

- SCHREINER, Rüdiger, 2019. *Computernetzwerke: von den Grundlagen zur Funktion und Anwendung* [online]. München: Hanser PDF e-Book. ISBN 978-3-446-46010-2. Verfügbar unter: https://doi.org/10.3139/9783446460102.
- SAUTER, Martin, 2018. *Grundkurs Mobile Kommunikationssysteme: LTE-Advanced Pro, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth* [online]. Wiesbaden: Springer Vieweg PDF e-Book. ISBN 978-3-658-21647-4. Verfügbar unter: https://doi.org/10.1007/978-3-658-21647-4.
- ECKERT, Claudia, 2018. *IT-Sicherheit: Konzepte - Verfahren - Protokolle* [online]. München: De Gruyter Oldenbourg PDF e-Book. ISBN 978-3-11-056390-0. Verfügbar unter: https://doi.org/10.1515/9783110563900.

- SCHÄFER, Günter und Michael ROßBERG, 2014. *Netzsicherheit: Grundlagen & Protokolle ; mobile & drahtlose Kommunikation ; Schutz von Kommunikationsinfrastrukturen*. 2. Auflage. Heidelberg: dpunkt-Verl.. ISBN 978-3-86490-115-7, 3-86490-115-4
- SORGE, Christoph, GRUSCHKA, Nils, LO IACONO, Luigi, 2013. *Sicherheit in Kommunikationsnetzen* [online]. München: Oldenbourg PDF e-Book. ISBN 978-3-486-72016-7, 3-486-72016-3. Verfügbar unter: http://www.degruyter.com/view/product/231461.
- SPITZ, Stephan, PRAMATEFTAKIS, Michael, SWOBODA, Joachim, 2011. *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen* [online]. Wiesbaden: Vieweg + Teubner PDF e-Book. ISBN 978-3-8348-1487-6, 978-3-8348-8120-5. Verfügbar unter: https://doi.org/10.1007/978-3-8348-8120-5.

Anmerkungen:

Keine Anmerkungen

Masterarbeit

Modulkürzel:	CASE_MA	**SPO-Nr.:**	13
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	3
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	Winter- und Sommersemester

Modulverantwortliche(r):	Apel, Sebastian
Leistungspunkte / SWS:	30 ECTS / 0 SWS
Arbeitsaufwand:	Kontaktstunden: 0 h Selbststudium: 750 h Gesamtaufwand: 750 h
Lehrveranstaltungen des Moduls:	Masterarbeit
Lehrformen des Moduls:	Prj - Projekt
Prüfungsleistungen:	Master-Abschlussarbeit
Verwendbarkeit für andere Studiengänge:	Keine

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Im Rahmen einer Master-Arbeit empfiehlt es sich, die Befähigung zu der wissenschaftlichen Arbeit unter anderem in Form einer soliden statistischen Auswertung zu demonstrieren. Daher sind Grundkenntnisse der deskriptiven und induktiven Statistik von Vorteil. Diesbezügliche Literaturhinweise zum Selbststudium finden Sie bei den Literaturangaben zu diesem Modul.

Angestrebte Lernergebnisse:

Nach der erfolgreichen Erstellung der Masterarbeit

- können die Studierenden ein Problem selbstständig und unter Einsatz wissenschaftlicher Methoden bearbeiten
- können die Studierenden Anforderungen, alternative Lösungsvorschläge sowie möglicherweise die Ausarbeitung einzelner Lösungsansätze bewerten und schriftlich in einer überzeugenden und nachvollziehbaren Weise darstellen
- haben die Studierenden gelernt, eine umfangreiche Aufgabenstellung durch effektives Zeitmanagement in einem vorgegebenen Zeitrahmen zum Abschluss zu bringen

Inhalt:

Eine Masterarbeit ist der wissenschaftliche Abschluss eines Studiums und Bestandteil der Prüfung. Sie soll zeigen, dass der Absolvent in der Lage ist, ein Problem aus seinem Studiengang selbstständig und unter Einsatz wissenschaftlicher Methoden zu bearbeiten.

Studenten erhalten hier die Gelegenheit, selbstständig eine Aufgabe zu bearbeiten, um damit Kreativität, aber auch den Willen und die Befähigung zur Bearbeitung und zum erfolgreichen Abschluss einer gestellten Aufgabe zu zeigen.

Die Erstellung einer Masterarbeit erfordert Können und Wissen auf vier Gebieten:

- Das jeweilige fachliche Wissen, welches zur Bearbeitung des Themas der Masterarbeit benötigt wird
- Techniken, Methoden und Vorgehensweisen des wissenschaftlichen Arbeitens
- Projektmanagement (insbesondere Zeitplanung und Controlling)
- gegebenenfalls Präsentationstechniken

Im Allgemeinen sucht sich der Studierende selbständig ein Thema für die Abschlussarbeit. Themen werden entweder hochschulintern von Professoren oder wissenschaftlichen Mitarbeitern der Hochschule in Aushängen (auch online) angeboten, oder ergeben sich aus der Kooperation des Studierenden mit einer externen Firma.

Im Fall einer externen Themenstellung muss der Studierende einen Dozenten der Hochschule von seinem Thema begeistern, damit dieser die Rolle des Erstprüfers übernimmt. Zu diesem Zweck empfiehlt es sich, die Themenstellung und die geplante Herangehensweise in einer kurzen Ausarbeitung zu skizzieren. Dieses Exposé dient dazu, den als Erstprüfer gewünschten Dozenten zu überzeugen.

Literatur:

Wird zu Beginn bekannt gegeben

Anmerkungen:

Keine Anmerkungen

5.2 Projekte

Projekt			
Modulkürzel:	CASE_PROJEKT	**SPO-Nr.:**	12
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Apel, Sebastian	
Leistungspunkte / SWS:	7 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	47 h
	Selbststudium:	129 h
	Gesamtaufwand:	176 h
Lehrveranstaltungen des Moduls:	Projekt	
Lehrformen des Moduls:	12: Prj - Projekt	
Prüfungsleistungen:	PA - Projektarbeit	
Verwendbarkeit für andere Studiengänge:	Keine	

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Im Rahmen des Projekts werden in der Regel Software-Komponenten oder ganze Anwendungen entwickelt. Daher sind solide Grundlagen auf folgenden Gebieten erforderlich: Programmierung (Java, Python, eventuell C/C++), Web-Programmierung (Java, PHP, ECMA), Datenbanksysteme, Netzwerktechnik, Revision Control (Git, Mercurial). Des Weiteren werden Kenntnisse auf dem Gebiet des agilen Projektmanagements (Scrum, Kanban) vorausgesetzt.

Angestrebte Lernergebnisse:

Nach erfolgreicher Teilnahme an den Lehrveranstaltungen

- haben die Studierenden die vertieften Kompetenzen zur praktischen Anwendung von Projektmanagementmethoden
- sind die Studierenden in der Lage versiert Werkzeuge, die im Rahmen der Durchführung eines IT-Projektes erforderlich sind, anzuwenden.
- können die Studierenden mit fachlichen und nicht-fachlichen Problemstellungen, die während der Durchführung eines mehrwöchigen Projektes auftreten können, umgehen und Lösungsstrategien identifizieren
- sind die Studierenden in der Lage, eine komplexe fachliche Aufgabenstellung zu analysieren und in der vorgegebenen Zeit in einem Team erfolgreich zu bearbeiten
- können die Studierenden in unterschiedlicher aber stets angemessener Ausführlichkeit über den Projektfortschritt in mündlicher und/oder schriftlicher Form berichten

- sind die Studierenden in der Lage, fachliche und nicht-fachliche (insbesondere auch unternehmerische) Ziele des Projekts kritisch zu hinterfragen und im Sinne eines Gesamterfolges des Projekts abzuwägen

Inhalt:

Bearbeitung einer semesterbegleitenden Projektaufgabe aus dem Bereich der Informatik mit Bezug zu Themen des Studiengangs in einem Team.

Im Allgemeinen werden die Projekte in Kooperation mit externen Firmen oder dem hochschuleigenen Forschungszentrum durchgeführt. Alternativ können auch Dozenten gezielt Projektthemen vorgeben, die im Rahmen ihrer Lehr- oder Forschungstätigkeit bearbeitet werden sollen.

Die Projektleitung und die Organisation werden von Studierenden ausgeführt. Der Dozent/Lehrbeauftragte fungiert als Coach und/oder Auftraggeber.

Als Projektmanagementmethode können klassische Methoden oder agile Methoden wie Scrum oder Kanban verwendet werden. Die Entscheidung darüber, welche Methode verwendet wird, liegt beim Projektteam.

Zu Beginn des Projekts kommuniziert der Dozent/Lehrbeauftragte klar seine Erwartungen hinsichtlich Termine, Form und Nachweis der individuellen Leistungen, die von allen Studierenden zu erbringen sind.

Das Projektteam einigt sich mit dem Dozenten/Lehrbeauftragten über die Kommunikations- und Dokumentationsformen, die während der Projektlaufzeit aller Projektteilnehmer (Studierende, Dozent, Auftraggeber) einzuhalten sind.

Zu klären sind:

- Häufigkeit und Dauer von Planungssitzungen
- Art und Durchführung der Treffen (gemeinsam oder virtuell/elektronisch)
- turnusmäßige Treffen (evtl. täglich in Form eines Scrum-Dailys)
- Art und Umfang der Deliverables
- Art und Umfang der individuellen Beträge durch Studierende
- Kriterien für die Beurteilung/Benotung durch den Dozenten

Literatur:

Wird zu Beginn bekannt gegeben

Anmerkungen:

Aus dem einschlägigen Bachelor-Studium werden Kenntnisse auf dem Gebiet Projektmanagement vorausgesetzt.

5.3 Seminare

Seminar			
Modulkürzel:	CASE_SEMI	**SPO-Nr.:**	11
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Art des Moduls**	**Studiensemester**
	Cloud Applications und Security Engineering (SPO WS 22/23)	Pflichtfach	2
Modulattribute:	**Unterrichtssprache**	**Moduldauer**	**Angebotshäufigkeit**
	Deutsch	1 Semester	nur Wintersemester

Modulverantwortliche(r):	Apel, Sebastian	
Leistungspunkte / SWS:	3 ECTS / 2 SWS	
Arbeitsaufwand:	Kontaktstunden:	23 h
	Selbststudium:	52 h
	Gesamtaufwand:	75 h
Lehrveranstaltungen des Moduls:	Seminar	
Lehrformen des Moduls:	11: S - Seminar	
Prüfungsleistungen:	SA - Seminararbeit mit Präsentation	
Verwendbarkeit für andere Studiengänge:	Keine	

Voraussetzungen gemäß SPO:

Keine

Empfohlene Voraussetzungen:

Im Rahmen der Seminarvorbereitung muss einschlägige Fachliteratur bearbeitet werden, die meistens in englischer Sprache vorliegt. Daher müssen die Teilnehmer in der Lage sein, englische Fachtexte aus dem Bereich der Informatik lesen zu können.

Angestrebte Lernergebnisse:

Nach dem Besuch des Moduls

- haben die Studierenden ihre Fähigkeit vertieft, sich selbständig spezielle fachliche Kenntnisse zu erarbeiten (Literaturarbeit, Analyse, Schlussfolgerungen) und können diese mithilfe des Einsatzes geeigneter Medien nachvollziehbar im Rahmen eines mündlichen Vortrags präsentieren
- sind die Studierenden in der Lage, einer fachlichen Präsentation kritisch zu folgen und die Inhalte mit dem Vortragenden fachlich zu diskutieren (Stärkung der kommunikativen Kompetenz)
- haben die Studierenden ihre überfachlichen und kommunikativen Kompetenzen verstärkt
- können die Studierenden den Inhalt ihrer Präsentation in Form einer kurzen schriftlichen Ausarbeitung darstellen

Inhalt:

Pro Semester werden im Allgemeinen mehrere Seminare angeboten. Gegenstand ist jeweils ein Themenfeld aus der aktuellen Forschung und Entwicklung im Kontext der angebotenen Studienschwerpunkte.

Der jeweilige Dozent stellt eine Sammlung von Papieren oder Bücher aus der Fachliteratur zusammen, die zugleich die Basisliteratur für die Vorträge darstellt.

Im Zuge des Seminars muss jeder Teilnehmer eine ganze Doppelstunde (90 Minuten) über ein Thema gestalten, welches ihm zu Beginn des Semesters per Los oder Wahl zugeteilt wird.

- In der Vorbereitungsphase muss jeder Teilnehmer Literaturrecherchen zu seinem Thema durchführen und deren Ergebnis in eine Präsentation einarbeiten.
- Diese Präsentation trägt er im Rahmen einer Doppelstunde mündlich vor. Der Vortrag soll ca. 60 Minuten dauern. Der Rest der Doppelstunde ist für die Diskussion des Vortrags vorgesehen.
- Zusätzlich ist eine schriftliche Ausarbeitung über das bearbeitete Thema zu erstellen. Diese Ausarbeitung soll die wesentlichen Inhalte des Vortrags in Prosa zusammenfassen und einen Umfang zwischen 5 und 10 Seiten haben (ohne Bilder und Verzeichnisse).

Detaillierte Hinweise zu Terminen und seine Erwartungen hinsichtlich der Gestaltung der Präsentation sowie der schriftlichen Ausarbeitung kommuniziert der jeweilige Dozent zu Beginn des Semesters.

Literatur:

Wird zu Beginn bekannt gegeben

Anmerkungen:

In diesem Modul besteht Anwesenheitspflicht.