Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modulhandbuch

Fakultät Informatik
Studiengang
Advanced IT Security M.Sc.

StuPO 21.2
ab Wintersemester 2021/22
Ersteller: Prof. Dr. German Nemirovski, Studiendekan
Verantwortlich: Prof. Dr. German Nemirovski, Studiendekan

Inhaltsverzeichnis

1 Vorwort

Der Masterstudiengang Advanced IT Security M.Sc. ist ein praxisorientierter Master-Studiengang. Die Inhalte werden auf wissenschaftlichem Niveau bei einer ausgeprägten Anwendungsorientierung vermittelt. Die Studierenden erlangen Qualifikationen, die sie befähigen, als technische Fach- und Führungskräfte, weltweit aber auch für die regionale mittelständische Industrie tätig zu sein. Die Fähigkeiten, Fertigkeiten und Kenntnisse der Absolventen ermöglichen ihnen die Übernahme von u.a der folgenden Positionen in der Industrie und in den Behörden:

- IT-Security-Experte
- System- und Softwareentwickler im Bereich IT Security
- Mitarbeiter im IT-Sicherheitsmanagement
- Mitarbeiter Incident Response Team
- Mitarbeiter im Bereich Pentesting und Security Audits
- Forensiker (Digitale Forensik)
- Leitender IT-Administrator

Folgende Qualifikationsziele werden in der Lehre gesetzt:

Sicherheitskompetenz
Die Studierenden sind in der Lage, im Rahmen einer eigenständigen Arbeit komplexe IT-Sicherheits- und -bedrohungsrelevante Fragen und Problemstellungen zu formulieren. Sie sind in der Lage mit analytischen Mitteln relevante Informationen zu Bedrohungen und Angriffen abzuleiten.
Methodenkompetenz
Die Studierenden verfügen über Kenntnisse von Methoden, Verfahren und Werkzeugen der IT-Sicherheit, darunter der Netzwerk- und Hardwaresicherheit, der digitalen Forensik, der Kryptographie und des Sicherheitsmanagements, und können diese in der Praxis anwenden.
Ferner können Studierende zweckdienliche Erkenntnisse auch aus anderen Wissenschaftsbereichen (z.B. Psychologie) und Anwendungsgebieten (z.B. IOT) zur Problemlösung heranziehen.
Ethische und Rechtliche Kompetenz
Die Studierenden sind in der Lage, ihr Vorgehen in einen rechtlich zulässigen, ethischen und moralischen Rahmen einzuordnen und kritisch zu hinterfragen. Insbesondere sind sie in der Lage, Datenerhebungs- und Datenverarbeitungsprozesse bezüglich Konflikten mit Datenschutz- und Persönlichkeitsrechten zu prüfen.
Konzeptionelle Fähigkeit
Die Studierenden sind in der Lage, eigenständig Konzepte und Analysen zu entwickeln. Besondere Bedeutung hat in diesem Zusammenhang die Fähigkeit, theoretische Konzepte auf die konkreten Anwendungsfälle zu übertragen.
Vernetztes Denken
Die Studierenden können Zusammenhänge aus unterschiedlichen Anwendungsgebieten innerhalb des Fachgebiets und in deren Umfeld herleiten. Sie sind in der Lage, fachübergreifend zu analysieren und Konzepte zu entwickeln.

Version	Geändert von Ammann/am 14.04.2021	Dokument	Freigabe am/von	Gültig ab WS 2021/22
1.0		Modulhandbuch_Advanced IT Security_Version1.0_Stand 20210414_final_QM_FINAL		

Forschungskompetenz
Im Bereich Wissenschaft und Forschung sind die Studierenden in der Lage, wissenschaftliche Methoden einzusetzen und die Forschungsergebnisse zielgruppengerecht aufzubereiten.

2 Übersicht der Modulbeschreibungen

2.1 1. Semester

xxxxx	Implementation Attacks and Countermeasures
Xxxxx	IT Security Management and Incident Response
51600	Open Source Intelligence
xxxxx	WPM 1a / WPM 1b

2.2 2. Semester

Xxxxx	Application Forensics
Xxxxx	Applied Cyberpsychology
Xxxxx	Human Factors in IT Security
xxxxx	WPM 2a / WPM 2b

2.3 3. Semester

60100	Master-Thesis

3 Qualifikationsziel-Modul-Matrix

Modul-Nr.	Modulbezeichnung	Qualifikationsziel (QuZ)	Summe der Unterstützungspunkte	Sicherheitskompetenz	Methodenkompetenz:	Ethische und Rechtliche Kompetenz:	Konzeptionelle Fähigkeit	Vernetztes Denken:	Forschungskompetenz:
XXX	Application Forensics		9	1	2	2	2	0	2
XXX	OSINT		8	1	2	2	0	2	1
XXX	Implementation Attacks and Countermeasures		9	2	2	1	2	1	1
XXX	IT Security Management and Incident Response		11	2	2	2	2	2	1
XXX	Applied Cyberpsychology		9	1	1	2	1	2	2
XXX	Human Factors in IT-Security		10	1	2	2	1	2	2
XXX	Wahlpflichtmodul 1a / 1b			X	X	X	X	X	X
XXX	Wahlpflichtmodul 2a / 2b			X	X	X	X	X	X
61000	Master Thesis			2	2	2	2	2	2

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

4 Studiengangs-Kompetenzmatrix

Kompetenzen		Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
Ausprägung		Tiefe	Breite	Instrumentelle Fertigkeiten	Systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit/ Verantwortung	Reflexivität	Lernkompetenz
51100	Application Forensics	7			7	7			7			7
52200	IT Security Management and Incident Response		7	7	7		7				7	
52300	Implementation Attacks and Countermeasures	7		7		7			7	7		
52700	Applied Cyberpsychology	7				7			7	7		
51500	Human Factors in IT-Security	7				7			7	7		
52100	OSINT	7	6	7	7	7			7	7		7
xxxxx	Wahlpflichtmodul 1a/1b	X	X	X	X	X	X	X	X	X	X	X
xxxxx	Wahlpflichtmodul 2a/2b	X	X	X	X	X	X	X	X	X	X	X
61000	Master Thesis	7	7	7	7	7	7	7	7	7	7	7

5 Modulbeschreibungen

5.1 1. Semester

5.1.1 xxxxx – Implementation Attacks and Countermeasures

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 / Version 1.0 **Letzte Bearbeitung**: 14.04.211

Modul: Implementation Attacks and Countermeasures						
Kennnummer z.B. 15100	**Workload** 180h	**Modulart** PM	**Studiensemester** 1. Semester	**Dauer** 1 Semester	**Häufigkeit** WS	
1	**Lehrveranstaltung(en)** Vorlesung Implementation Attacks and Countermeasures Projekt Implementation Attacks and Countermeasures		**Sprache** Deutsch oder Englisch	**Kontakt-zeit** 4 SWS / 60h	**Selbst-studium** 120	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** Vorlesung Implementation Attacks and Countermeasures / 2 SWS Projektarbeit Implementation Attacks and Countermeasures / 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden können Seitenkanal-, und Fehler-Angriffe, sowie geeeignete Gegenmaßnahmen verstehen und die Bedrohungslage durch solche Angriffe adäquat einschätzen. [Wissen, 7]					
	Kompetenz Fertigkeiten Die Studierenden können Seitenkanal- und Fehler-Angriffe durchführen, sowie geeignete Gegenmaßnahmen implementieren. Dabei können die Studierende die Notwendigkeit und Auswahl der Gegenmaßnahmen an die Anwendung und die daraus resultierende Bedrohungslage anpassen. *[Instrumentelle Fertigkeiten, 7]* Die Studierenden können die Sicherheit von Software und Hardware bezüglich Implementierungs-Angriffe beurteilen und Schwachstellen in Implementierungen aufdecken, sowie Gegenmaßnahmen entwickeln. *[Beurteilungsfähigkeit, 7]*					
	Sozialkompetenz Die Studierenden können komplexe statistische und andere Sachverhalte zu Implementierungs-Angriffen mit anderen Experten diskutieren und weiterentwickeln, sowie die Notwendigkeit von geeigneten Gegenmaßnahmen kompetent und zielgruppengerecht vermitteln.. *[Kommunikation, 7]*					

	Selbstständigkeit Die Studierenden können selbstständig komplexe Zusammenhänge der IT-Sicherheit verstehen, beurteilen und daraus geeignete Maßnahmen eigenverantwortlich ableiten. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte***:* Vorlesung - Physikalische Grundlagen von Seitenkanal-Angriffen - Statistische Grundlagen der Seitenkanalanalysen - Simple Power Analysis, Differential Power Analysis, Timing Attacks - Vertikale und Horizontale Angriffe gegen Public Key Kryptografie - Microarchitekturelle Angriffe - Grundlegende Einführung zu Seitenkanal-Gegenmaßnahmen - Masking und Higher-Order Masking von kryptografischen Algorithmen - Hiding-Maßnahmen - Gegenmaßnahmen für Public Key Kryptografie, wie z.B.Scalar Blinding, oder Point Randomization - Konstruktive Maßnahmen, wie z.B. statistische Leakage-Detektion - Physikalische Grundlagen für Fehlerangriffe - Voltage-Glitch-Angriffe, Clock-Glitch-Angriffe, Laser-Fault Injection, EM-Fault Injection - Beobachtbare Fehlerbilder und Ausnutzung der Fehler in unterschiedlichen Szenarien - Gegenmaßnahmen wie Redundanz, Glitch-Detektoren, oder Laser-Detektoren Projekt - Praktische Umsetzung und Evaluation von ausgewählten Angriffen und Gegenmaßnahmen
	Empfohlene Literaturangaben: Mangard, S., Oswald, E., Popp, T. - Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer-Verlag, 2007 Kocher, P., Jaffe, J., Jun B. - Differential Power Analysis, CRYPTO '99, Springer-Verlag, 1999 Gilbert Goodwill, B. J., Jaffe, J., Rohatgi, P. - A testing methodology for side-channel resistance validation, NIST Non-invasive Attack Testing Workshop, Vol. 7, pp. 115-136, 2011 Kocher P., Horn J., Fogh A., Genkin D., Gruss D., Haas W., Hamburg M., Lipp M., Mangard S., Prescher T., Schwarz M., Yarom Y. - Spectre Attacks: Exploiting Speculative Execution, IEEE S & P, 2019
5	**Teilnahmevoraussetzungen:** Grundlagen der Kryptotolgie, Statistische Grundlagenkenntnisse, Programmierkenntnisse (idealerweise in ARM-Assembler oder VHDL)
6	**Prüfungsformen***:* Referat 20 min., Diskussion, benotet

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Ausarbeitung Ausreichend bewertetes Referat
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.2 xxxxx - IT Security Management and Incident Response

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 18.03.2021

<table>
<tr><td colspan="8">Modul: IT Security Management and Incident Response</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
180 h</td><td>Modulart
PM</td><td colspan="2">Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. Vorlesung, Advanced IT Security Management
b. Projekt Incident Response</td><td>Sprache
Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, Seminar Advanced IT Security Management: 2 SWS
b. Vorlesung, Praktikum Incident Response: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden können die gesetzlichen Grundlagen und „Best Practice“ Methoden des IT-Sicherheitsmanagements (ISM) erklären. [Wissen, 7]
Die Studierenden können die Voraussetzungen für eine Incident Response nennen und die verschiedenen Phasen einer Incident Response erläutern. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können ein Konzept für die Einrichtung eines ISM erstellen und umsetzen sowie ein bestehendes ISM anhand nationaler und internationaler Standards bewerten. [Instrumentelle Fertigkeiten, 7]

Die Studierenden können ein Incident Response Team etablieren und die einzelnen Phasen einer Incident Response durchführen. [Systemische Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden können sich auf Expertenebene mit der Fachcommunity über Methoden und Werkzeuge des IT-Sicherheitsmanagements unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln [Kommunikation, 7]

Die Studierenden können Laien für Fragen der IT-Sicherheit interessieren, die Notwendigkeit von Maßnahme der IT-Sicherheit darstellen und erläutern, und IT Sensibilisierungskampagnen im Bereich der IT-Sicherheit planen und durchführen. [Team-/Führungsfähigkeit, 7]

Selbstständigkeit
Die Studierenden können den Umsetzungsgrad des ISM reflektieren und bei Änderungen der Rahmenbedingungen gegebenenfalls Änderungsbedarf erarbeiten,</td></tr>
</table>

	darstellen und umsetzen. [Reflexivität, 7] Die Studierenden die Fähigkeiten zur Incident Response unter Berücksichtigung der Bedrohungslage reflektieren und anpassen. [Reflexivität, 7]
4	**Inhalte*:*** Vorlesung, Seminar Advanced IT-Sicherheitsmanagement: • Auffrischung IT-Sicherheitsmanagement • Compliance, nationale und internationale Standards für IT-Sicherheitsmanagement • Sensibilisierung Vorlesung, Praktikum Incident Response • Auffrischung IT-Sicherheitsmanagement, Digitale Forensik • Voraussetzungen für Incident Response • Phase von Incident Response • Intrusion Detection Systems
	Empfohlene Literaturangaben:
5	**Teilnahmevoraussetzungen:** Grundlagen der IT-Sicherheit, Programmierkenntnisse
6	**Prüfungsformen***:* Referat 20 min. inkl. wissenschaftlicher Ausarbeitungen, Diskussion, benotet Laborarbeit, unbenotet
7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Ausreichend bewertetes Referat erfolgreiche Teilnahme am Praktikum
8	**Verwendbarkeit des Moduls:** Advanced IT Security M.Sc.
9	**Modulverantwortliche(r):** Prof. Dr. Henrich Dozent: Prof. Dr. Henrich
10	**Optionale Informationen:** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.3 51600 – Open Source Intelligence

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="7">Modul: Open Source Intelligence</td></tr>
<tr><td colspan="2">Kennnummer
51600</td><td>Workload
180 h</td><td>Modulart
PM</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Open Source Intelligence
Praktikum Open Source Intelligence</td><td>Sprache
Deutsch oder Englisch (Literatur-studium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Übungen, Seminar: 3 SWS
Praktikum: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verfügen über ein breites Wissen über die technischen, gesellschaftlichen und rechtlichen Rahmenbedingungen für einen OSINT Einsatz, [Wissen, 6]
Die Studierenden verfügen über ein tiefes Wissen im Bereich von OSINT Terminologien, Methoden und Techniken, [Wissen, 7]

Kompetenz Fertigkeiten
Können einen OSINT Einsatz konzeptionell strukturieren und geeignete Methoden und Werkzeuge auswählen [Instrumentelle Fertigkeiten, 7]

Können die Leistungsfähigkeit vorhandener OSINT Werkzeuge beurteilen und selbstständig neue OSINT Verfahren und Werkzeuge entwickeln [Systemische Fertigkeiten, 7]

Können per OSINT ermittelte Daten hinsichtlich ihrer technischen und juristischen Verwertbarkeit beurteilen und ihren Informations- und Intelligence Gehalt einschätzen [Beurteilungsfähigkeit, 7]

Sozialkompetenz
Studierende können sich auf tiefer Expertenebene mit der Fachcommunity unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln [Kommunikation, 7]

Selbstständigkeit</td></tr>
</table>

	Studierende können neue OSINT Anwendungen eigenständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren *[Eigenständigkeit/Verantwortung, 7]* Aktuelle Aufgabenstellungen und Probleme aus dem OSINT Bereich können eigenständig anhand der aktuellen Forschung im Print- und Preprintbereich erschlossen werden *[Lernkompetenz, 7]*
4	**Inhalte*:*** Vorlesung, Seminar, Praktikum • Auffrischung relevanter Grundlagen der IT Sicherheit, Digitalen Forensik und Internettechnologien • Anonymisierung und De-Anonymisierung im Surface-, Deep- und Darknet • Ermittlungstaktisches- / nachrichtendienstliches Vorgehen • OSINT Grundlagen, Terminologien, Taxonomien • OSINT Methoden, Tools, Techniken • Legaler, moralischer und ethischer Rahmen • Analyse und Bewertung von OSINT Erkenntnissen • Praktische Anwendungen • Wissenschaftliche Recherche, Arbeit und Forschung im OSINT Bereich • Relevante wissenschaftliche Konferenzen, Journals und Plattformen
	Empfohlene Literaturangaben: Akhgar, B., Bayerl, P.S., Sampson, F.S.: OpenSource Intelligence Investigation – From Strategy to Implementation, Springer, 2017 Bazzell, M.: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 5. Auflage, CreateSpace Independent Publishing Platform, 2016 U.S.Army: NATO OpenSource Intelligencehandbook, online, http://www.au.af.mil/au/awc/awcgate/nato/osint_hdbk.pdf Attrill, A.: Cyberpsychology, 2015, Oxford University Press Gollmann, D.: Computer Security, 3. Auflage, Wiley, 2012 Tavani, H.T.: Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, 4. Auflage, Wiley, 2013 Spinello, R.: Cyberethics: Morality and Law in Cyberspace 6th Edition, Jones & Bartlett Learning, 2016 A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology, 5th Edition, Pearson, 2017 Biskup, J.: Security in Computing Systems, Springer, 2010 Ausgewählte Literatur bekannter Top-Tier Konferenzen im OSINT Bereich Weitere Literatur wird in der Vorlesung vorgestellt.
5	**Teilnahmevoraussetzungen:** Grundlagen Betriebssysteme und Netzwerke, Grundlagen IT Sicherheit und Digitaler Forensik, Programmierung in einer Skriptsprache
6	**Prüfungsformen***:* Referat 20 min. inkl. wissenschaftlicher Ausarbeitungen und Poster, Diskussion, benotet Laborarbeit, unbenotet

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Morgenstern Dozenten: Prof. Dr. Fein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.4 xxxxx – Wahlpflichtmodul 1a / Wahlpflichtmodul 1b

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 / Version 1.0 **Letzte Bearbeitung**: 14.04.211

<table>
<tr><td colspan="7">Modul: Wahlpflichtmodule 1a / 1b</td></tr>
<tr><td colspan="2">Kennummer</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog (extra Liste)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
12</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Wird definiert durch jeweiligen Modulverantwortlichen</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen [Systemische Fertigkeiten, 7]

Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. [Team-/Führungsfähigkeit, 7]

Selbstständigkeit
Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Für die hier Wahlpflichtmodulteile existieren jeweils gesonderte Modulteilbeschreibungen in diesem Modulhandbuch. Wenn Modulteile aus anderen Masterstudiengängen gewählt werden gelten die Inhaltsangaben der dort definierten Modulteilbeschreibungen. Sofern in diesen Fällen grundlegende Vorkenntnisse erforderlich sind die im bisherigen Studienverlauf der Studierenden nicht zwangsläufig erworben wurden, obliegt es dem Kandidaten diese Vorkenntnisse gesondert zu erwerben

Empfohlene Literaturangaben:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
</table>

5	**Teilnahmevoraussetzungen:** Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)
6	**Prüfungsformen***:* Siehe jeweilige Modulteilbeschreibungen
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Es gelten die Ausführungen in den Beschreibungen des WPM
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozenten: s. Modulbeschreibungen der jeweiligen WPM
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2 2. Semester

5.2.1 xxxxx – Application Forensics

Studiengang: Advanced IT Security M.Sc.
StuPO-Version: 21.2

Semester: WS 2021/22
Letzte Bearbeitung: 14.04.21

<table>
<tr><td colspan="8">Modul: Application Forensics</td></tr>
<tr><td colspan="2">Kennnummer:
52600</td><td>Work-load
180 h</td><td>Modulart
PM</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td colspan="2">Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung/Seminar Application Forensics
Projekt Application Forensics</td><td>Sprache
Deutsch oder Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td colspan="2">Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung, Übungen, Seminar: 2 SWS
Projekt: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verfügen über grundlegende Methoden und spezialisierte Techniken zur forensischen Analyse von digitalen Anwendungsspuren [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in der Lage neue Verfahren zur Analyse neuer Applikationen zu entwickeln. [Systemische Fertigkeiten, 7]
Analyseergebnisse können unter verschiedenen Maßstäben beurteilt werden. [Beurteilungsfähigkeit, 7]
Sozialkompetenz
Die Ergebnisse einer komplexeren forensischen Anwendungsanalyse können einem Fachpublikum vorgestellt und mit ihm diskutiert werden. [Kommunikation, 7]
Selbstständigkeit
Analysemethoden und Techniken zur Untersuchung unbekannter Applikationen kann selbstständig erschlossen werden. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Vorlesung, Seminar, Projekt
• Auffrischung relevanter Grundlagen der IT Sicherheit, Digitalen Forensik</td></tr>
</table>

	• Einführung Anwendungsforensik • Methoden der Anwendungsforensik • Legaler und ethischer Rahmen • wissenschaftliches Arbeiten und Berichten • Praktische Anwendungsanalyse • wissenschaftlicher Fachvortrag
	Empfohlene Literaturangaben: • Andreas Dewald, Felix Freiling: Forensische Informatik. Books on Demand, 2. Auflage, 2015 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Grundlagen Betriebssysteme und Netzwerke, Grundlagen IT Sicherheit und Digitaler Forensik, Programmierung in einer Skriptsprache (vorz. Python)
6	**Prüfungsformen***:* Referat 30 min. inkl. wissenschaftlicher Ausarbeitungen und Poster, Diskussion, benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat erfolgreiche Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Morgenstern Prof. Dr. Fein Dozenten: Prof. Morgenstern, Prof. Dr. Fein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.2 xxxxx – Applied Cyberpsychology

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 18.03.2021

<table>
<tr><td colspan="7">Modul: Applied Cyberpsychology</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
180 h</td><td>Modulart
PM</td><td>Studien-semester
2. Semester</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
a.Vorlesung Applied Cyberpsychology
b.Projekt</td><td>Sprache
englisch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
a.Vorlesung mit Übungen / 2 SWS
b.Projekt / 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Lernergebnisbeschreibung einer bestimmten Kompetenz z.B. Fachwissen mit Niveaustufe Die Studierenden besitzen ein breites Wissen über Anwendungen psychologischer Methodik und Erkenntnisse im Bereich der Cyberpsychologie.
Die Studierenden besitzen ein Überblick über die Anwendungsmöglichkeiten psychologischer Prinzipien und Methoden im Bereich der IT-Security. Die Studierenden sind vertraut mit den Grundlagen organisationspsychologischer Prinzipien und Entscheidungsprozessen in normalen und kritischen Situationen sowie der Kommunikation in komplexen sozioteschnischen Systemen und interdisziplinärer Kooperation. [Wissen, 7]

Kompetenz Fertigkeiten
Selbstständiger Wissenserwerb zu verhaltensrelevanten Problemen und Problemlösungsansätzen unter Verwendung wissenschaftlicher Primärquellen. Kritisches Beurteilen und theoretisches sowie methodisches Einordnungen neuerer wissenschaftlicher Erkenntnisse. [Instrumentelle Fertigkeiten, 7]

Sozialkompetenz
Studierende können interdisziplinär schriftlich und mündlich verständlich kommunizieren und so zu gemeinsamer Problemlösung beitragen. Erkenntnisse und Methoden diskutieren und ihr Expertenwissen interdisziplinären Communities vermitteln. Fachwissen externer internationaler Experten kann zielgerichtet erlangt, verarbeitet und in vorhandenes Wissen integriert werden. [Kommunikation, 7]

Selbstständigkeit
Studierende erkennen eigenständig Anwendungsgebiete verhaltenswissenschaftlicher Methoden und Prinzipien und nutzen ihre Kenntnisse</td></tr>
</table>

	zur Leistungsverbesserungen bei sich selbst und anderen. Sie können forschungsmethodische Instrumentarien selbstständig auswählen und anwenden. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** Biopsychosocial concepts of perception, cognition and action Decision-making in digital and hybrid environments Performance under pressure Expertise and accelerated learning Foundations of behavior change and teaching concepts Principles of organizational psychology Particularities of human behavior in virtual environments and anonymity/pseudonymity Macrocognition and group effects in online communities and social influences Principles of neuro-ergonomics and neurocognition Motivation, emotions and decision-making Interdisciplinary cooperation and leadership styles, team communication
	Empfohlene Literaturangaben: Empfohlene Literaturangaben
5	**Teilnahmevoraussetzungen:** Aufnahme Master Advanced IT-Security M.Sc.
6	**Prüfungsformen***:* Mündliche Prüfung 20 Minuten
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Prüfung
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Sütterlin Dozenten: Prof. Dr. Sütterlin
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.3 xxxxx – Human Factors in IT Security

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 18.03.2021

<table>
<tr><td colspan="7">Modul: Human Factors in IT Security</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
180 h</td><td>Modulart
PM</td><td>Studiensemester
2. Semester</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
a.Vorlesung Human Factors in IT Security
b.Projekt</td><td>Sprache
englisch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
a.Vorlesung mit Übungen / 2 SWS
b.Projekt / 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen die Grundlagen der Human Factors Forschung im Bereich der IT-Security. Sie sind vertraut mit der wissenschaftlichen Literatur im inhaltlichen und methodischen Sinne.
Die Studierenden kennen die relevanten Modelle und Theorien zur Erklärung des Zusammenhangs zwischen menschlichem Erleben und Verhalten und Implikationen für IT-Sicherheit. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, in sicherheitsrelevanten sozio-technischen Systemen menschliche Risikofaktoren für die IT-Sicherheit zu erkennen, zu quantifizieren, interdisziplinär zu vermitteln und Vorschläge zu entwickeln. Sie sind in der Lage, selbstständig sicherheitsrelevante Fragen mit Hilfe verhaltenswissenschaftlicher Merthodik zu operationalisieren und durchzuführen und die Ergebnisse kritisch zu interpretieren. [Beurteilungsfähigkeit, 7]

Sozialkompetenz
Die Studierenden sind in der Lage, mit internationalen Experten in englischer Sprache fachspezifische Themen auf hohem Niveau zu diskutieren, die gewonnenen Informationen zu verarbeiten und vor einem Fachpublikum zu präsentieren. [Kommunikation, 7]

Selbstständigkeit
Die Studierenden verstehen das Lernen als einen komplexen Prozess der die Recherche, das Verständnis und die Verarbeitung von Informatione interdisziplinären Ursprungs beinhaltet. Sie verfügen über die Motivation und</td></tr>
</table>

	Ausdauer um sich in ungewohnte Themengebiete einzuarbeiten und schriftlich auf wissenschaftlichem Niveau auszutauschen. *[Lernkompetenz, 7]*
4	**Inhalte*:*** Psychological aspects of cybercrime Internal threats Social Engineering Dark Patterns Expertise and indicators of performance Typologies, profiles and motivations of perpetrators Security awareness and interventions Cooperation and communication of IT-security threats and incidents Ergonomic aspects of IT-security behaviour and interface design Gamification approaches to improved IT-security behavior Research Methods for IT-security Recruiting, assessment, performance monitoring, predictors of success
	Empfohlene Literaturangaben: Empfohlene Literaturangaben
5	**Teilnahmevoraussetzungen:** Aufnahme Master Advanced IT-Security M.Sc.
6	**Prüfungsformen***:* Mündliche Prüfung, 20 min.
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Prüfung
8	***Verwendbarkeit des Moduls:*** Master Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Sütterlin
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.4 xxxxx – Wahlpflichtmodul 2a / Wahlpflichtmodul 2b

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 / Version 1.0 **Letzte Bearbeitung**: 14.04.211

<table>
<tr><td colspan="7">Modul: Wahlpflichtmodule 2a / 2b</td></tr>
<tr><td colspan="2">Kennnummer</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog (extra Liste)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Wird definiert durch den jeweiligen Modulverantwortlichen</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen [Systemische Fertigkeiten, 7]

Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. [Team-/Führungsfähigkeit, 7]

Selbstständigkeit
Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Für die hier Wahlpflichtmodulteile existieren jeweils gesonderte Modulteilbeschreibungen in diesem Modulhandbuch. Wenn Modulteile aus anderen Masterstudiengängen gewählt werden gelten die Inhaltsangaben der dort definierten Modulteilbeschreibungen. Sofern in diesen Fällen grundlegende Vorkenntnisse erforderlich sind die im bisherigen Studienverlauf der Studierenden nicht zwangsläufig erworben wurden, obliegt es dem Kandidaten diese Vorkenntnisse gesondert zu erwerben

Empfohlene Literaturangaben:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
</table>

5	**Teilnahmevoraussetzungen:** Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)
6	**Prüfungsformen***:* Siehe jeweilige Modulteilbeschreibungen
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Es gelten die Ausführungen in den Beschreibungen des WPM
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozenten: s. Modulbeschreibungen der jeweiligen WPM
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.3 3. Semester

5.3.1 60100 – Master-Thesis

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="7">Modul: Master-Thesis</td></tr>
<tr><td colspan="2">Kennnummer
60100</td><td>Work-load
750 h</td><td>Modulart
PM</td><td>Studiensemester
3</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Projekt Master-Thesis
Mündliche Prüfung
Kolloquium</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
--</td><td>Selbst-studium
750 (Präsenz & Selbst-studium)</td><td>Credits (ECTS)
25</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Projekt, betreute selbständige wissenschaftliche Arbeit</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Abhängig vom Thema der Masterarbeit [Wissen, 7]

Kompetenz Fertigkeiten
Mit der Master – Thesis zeigt der Student, dass er unter Anleitung selbständig umfangreiche wissenschaftliche Themen bearbeiten kann. Er wird praxisorientierte oder theoretische Themenstellungen nach wissenschaftlichen Kriterien analysieren, strukturieren und ergebnisorientiert bearbeiten. Die Master – Thesis dokumentiert seine Arbeit und erfüllt die Kriterien eines wissenschaftlichen Berichts. [Systemische Fertigkeiten, 7]

Sozialkompetenz
Abhängig vom Thema und Ort der Ausarbeitung (z.B. ein externes Unternehmen) 7]

Selbstständigkeit
Master-Thesis ist das größte Projekt im gesamten Master-Studiums, das die Studierenden nachweislich selbständig und verantwortlich ausführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
abhängig von Thema und Inhalt der Master-Thesis

Empfohlene Literaturangaben:
Abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
</table>

5	**Teilnahmevoraussetzungen:** Ggf. formal geregelt in der Prüfungsordnung
6	**Prüfungsformen***:* Master-Thesis (Ma.), benotet. Mündliche Prüfung 20 min., benotet Referat 25 Min, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen die Masterthesis (schriftliche Ausarbeitung). Bestehen die mündliche Prüfung, Bestehen das Referat
8	***Verwendbarkeit des Moduls:*** Advanced IT Security, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: abhängig vom Thema und Inhalt der Master-Thesis
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul