Modulhandbuch

Fernstudium

Master
IT-Sicherheit und Forensik

Stand: 03.11.2023

WINGS-FERNSTUDIUM
AN DER HOCHSCHULE WISMAR

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

Inhaltsverzeichnis

Modulbezeichnung Deutsch: Einführung in die IT-Sicherheit und Forensik	
Modulbezeichnung Englisch: Introduction to IT-Security and Digital Forensic Science	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	• Aktuelle Probleme der IT-Sicherheit und Forensik (Motivation) • Überblick über Institutionen, rechtliche Rahmenbedingungen und Informationsquellen zum Thema IT-Sicherheit und Forensik • Überblick über das IT-Sicherheitsgesetz, der IT-Sicherheitsstandards und der IT-Sicherheitsempfehlungen des BSI • Kennenlernen des IT-Sicherheitsprozesses • Vermittlung von Wissen über die Erstellung einer IT-Sicherheitskonzeption und des IT-Sicherheitsmanagement sowie des Risikomanagements • Kennenlernen von Beispiel-Szenarien zur IT-Sicherheit in speziellen Anwendungskontexten • Kennenlernen der Ziele, des Anliegens und der Probleme in der IT-Forensik • Beispiele zu IT-Forensischen Untersuchungen und IT-Forensischen Berichten • Kennenlernen des forensischen Prozesses • Vermittlung von Überblickswissen über Teilgebiete der IT-Forensik (Datenträger-, Betriebssystem-, Netzwerk-, Mobile, Big Data-, Browser-Forensik, Forensik in IT-Anwendungen, u.a.)
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden sind nach erfolgreichem Abschluss des Moduls für die Fragestellungen, rechtlichen Rahmenbedingungen und Probleme der IT-Sicherheit und der IT-Forensik sensibilisiert. Sie haben Grundkenntnisse im Sicherheitsmanagement, des Risikomanagements und der Sicherheitsanalyse. Die Studierenden kennen die allgemeinen Maßnahmen, die bei einer IT-forensischen Untersuchung zu beachten sind und kennen die Anforderungen an eine IT-forensische Dokumentation. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden können IT-Sicherheitsprobleme klassifizieren und sind in der Lage diejenigen forensischen Vorgänge zu identifizieren, die eine detailliertere IT-forensischen Analyse benötigen. <u>Kommunikation und Kooperation</u> Die Fernstudierenden organisieren sich in Gruppen und

	tauschen sich kritisch über Fachaspekte aus. Sie haben eine Kultur der virtuellen Zusammenarbeit etabliert. <u>Wissenschaftliche Selbstverständnis/ Professionalität</u> Die Studierenden sind in der Lage, sich selbständig neues Wissen anzueignen. Sie haben sich ein berufliches Selbstbild erarbeitet.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik und Informatik
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung: Präsentation und schriftliche Ausarbeitung oder 120-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	1. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Netzwerk- und Sicherheitsmanagement	
Modulbezeichnung Englisch: Network and Security Management	
Modulverantwortliche(r)	Prof. Dr. Nils Gruschka
Inhalte des Moduls	• Sicherheitsprobleme und Angriffe in Netzwerken • Angewandte Kryptographie • Transport-Layer-Security • DNS-Sicherheit • Web-Sicherheit • Sicherheit in lokalen Netzen (Firewalls, VPN, IDS) • WLAN-Sicherheit
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls vertiefte Kenntnisse über Angriffsmechanismen und sicherheitsrelevanten Aspekte in vernetzten Rechnersystemen und können diese klassifizieren und bewerten. Die Studierenden verstehen die Mechanismen und Strategien zur Erhöhung der Sicherheit von Rechnernetzen und können deren Folgen kritisch reflektieren. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden sind befähigt, die Sicherheitsarchitektur vernetzter Rechnersysteme zu bewerten und Forschungsfragen aufzuwerfen. Sie können die Mechanismen/ Strategien zur Erhöhung der Sicherheit von Rechnernetzen auch in neuen, unbekannten Umgebungen anwenden. Sie sind weiterhin zur Administration sicherheitsspezifischer Mechanismen in Rechnernetzen befähigt. <u>Kommunikation und Kooperation</u> Die Studierenden haben gelernt, virtuelle Gruppenprojekte zu ausgewählten Themen zu organisieren und sich die Inhalte zu erarbeiten. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden sind in der Lage, das eigene berufliche Handeln bzgl. der Sicherheit in Rechnernetzen mit theoretischem und methodischem Wissen zu begründen und reflektieren es hinsichtlich alternativer Entwürfe.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und aktueller Literatur; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen

Voraussetzung für die Teilnahme	Grundkenntnisse in Informatik, Mathematik, Betriebssysteme, Kommunikationstechnik
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	1. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Kryptografische Methoden und Anwendungen	
Modulbezeichnung Englisch: Cryptographic Methods and Applications	
Modulverantwortliche(r)	Prof. Dr.-Ing. habil. Andreas Ahrens
Inhalte des Moduls	• Einführung in die mathematischen Grundlagen und Konzepte der klassischen und modernen Kryptologie sowie in Grundwissen über deren Algorithmen, Protokolle und Verfahren • Beschreibung und Behandlung symmetrischer und asymmetrischer Verschlüsselungsverfahren und digitaler Zertifikate • Kryptografische Anwendungen: Diffie-Hellman Schlüsselaustausch, ElGamal Verschlüsselung, Signaturen
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls Kenntnisse über grundlegende Probleme der IT-Sicherheit und deren Zusammenhang zur Verschlüsselungsproblematik. Sie lernen wichtige kryptografische Verfahren und deren mathematische Grundlagen kennen. Sie sind in der Lage Besonderheiten, Grenzen, Terminologien und Lehrmeinungen des Lehrgebiets zu definieren und zu interpretieren. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptografie eingesetzt werden und können diese anhand von symmetrischen und asymmetrischen Verfahren nachvollziehen. Die Studierenden sind befähigt, Techniken zur Konstruktion und Analyse ausgewählter komplexer kryptografischer Algorithmen eigenständig auch in neuen Situationen anzuwenden. Sie sind in der Lage, wissenschaftlich fundierte Entscheidungen zu kryptografischen Verfahrungen zu treffen und reflektieren kritisch mögliche Folgen. <u>Kommunikation und Kooperation</u> Die Studierenden haben gelernt, sich sach- und fachbezogen untereinander über alternative, theoretisch begründbare Problemlösungen auszutauschen. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden sind in der Lage, das eigene berufliche Handeln bzgl. des Einsatzes von kryptografischen Verfahren mit theoretischem und methodischem Wissen zu begründen und reflektieren es hinsichtlich alternativer Möglichkeiten. Darüber hinaus besitzen die Studierenden alle

	Voraussetzungen neue symmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen einzuschätzen.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik, Informatik und Programmierung
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung (25%) und 90-minütige schriftliche Prüfung (75%)
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	1. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Rechtliche Grundlagen der IT-Sicherheit und Forensik	
Modulbezeichnung Englisch: Legal Foundations of IT-Security and Digital Forensic Science	
Modulverantwortliche(r)	Prof. Dr. jur. habil. Marina Tamm
Inhalte des Moduls	• Einführung in die nationalen und europäischen Grundlagen des Datenschutzrechts • deutsches und europäisches Grundrecht auf informationelle Selbstbestimmung und auf Integrität computergestützter Systeme, nationale und europäische Bestimmungen zum Datenschutz inkl. der einschlägigen Rechtsprechung • internationale Vorgaben zum Datenschutz (insbesondere Datenschutzabkommen mit Drittstaaten) • aktuelle Justizkonflikte etwa im Zusammenhang mit der Vorratsdatenspeicherung • Bestimmungen des materiellen Strafrechts in Cybercrime-Delikten • Urheberrechtliche Fragestellungen
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls die Befähigung zur Anwendung polizeilicher bzw. strafverfolgungsrechtlicher Handlungsbefugnisse im Grenzbereich zum Datenschutzrecht. Sie haben Wissen über datenschutzrechtlichen Vorgaben des Verfassungsrechts sowie des deutschen und europäischen Sekundärrechts und Wissen um internationale Abkommen zum Datenschutz sowie den diesbezüglichen Anwendungsvorgaben der Rechtsprechung. Die Studierenden kennen das juristische Fachvokabular zu den o.g. Aspekten. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden können IT-sicherheitskritische Vorfälle juristisch einordnen und juristische Aspekte in forensische Berichte integrieren. Sie sind befähigt, ausgewähltes juristisches Fachvokabular adäquat einzusetzen. <u>Kooperation und Kommunikation</u> Die Studierenden haben eine fachübergreifende (Informatik-Recht) Kommunikationskultur entwickelt. Sie sind in der Lage, technische und juristische Aspekte in Diskussionen zur IT-Sicherheit einzubringen und die unterschiedlichen Sichtweisen in Diskussionen zu respektieren. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u>

	Die Studierenden sind befähigt, ihr berufliches Handeln in Bezug auf gesellschaftliche Erwartungen und Folgen zu reflektieren und entwickeln ihr berufliches Handeln entsprechend weiter.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	1. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Angewandte biometrische Systeme	
Modulbezeichnung Englisch: Applied Biometric Systems	
Modulverantwortliche(r)	Prof. Dr.-Ing. Matthias Kreuseler
Inhalte des Moduls	• Einführung in biometrische Verfahren und Systeme (Grundbegriffe: Verifikation, Identifikation, FRR, FAR, EER) • Detaillierte Vermittlung der drei derzeit am stärksten verbreiteten Verfahren: Fingerabdruckerkennung, Gesichtserkennung und Iriserkennung • Multi-Biometrie: Ansätze zur Fusionierung der Matching-Scores unterschiedlicher Biometrien • Risikobehandlung und Grundprinzipien des Datenschutzes beim Umgang mit Biometriedaten • Grundprinzipien der Fälschungserkennung • Templateschutz und erneuerbare Biometrietemplates (Grundprinzipien der Templatetransformation und biometrischer Kryptosysteme) Biometrische Standards und Standarddatenformate (BioAPI 2.0, CBEFF, ISO 19794, NIST) • Wichtige ausgewählte biometrische Anwendungen (eBorder – elektronische biometrische Grenzsysteme, mobile biometrische Personenverifikation, biometrische Wählerregistrierung) • Aktuelle Trends: biometrische Verifikation „On the Move“ Finger- oder Iriserkennung aus der Bewegung heraus
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls fundiertes Wissen über wichtige biometrische Basisprozesse (Enrolment, Merkmalsextraktion, Matching) und verstehen die standardisierte Referenzarchitektur biometrischer Systeme. Sie kennen die wichtigsten biometrischen Verfahren, wie Fingerabdruck-, Gesichts- und Iriserkennung und beherrschen wichtige Größen zur Bewertung von Performance und Sicherheit von Biometriesystemen. Dieses Wissen, das signifikant über die Bachelorebene hinausgeht, versetzt sie in die Lage, Grenzen und Schwachstellen aktueller Systeme zu erkennen und wissenschaftlich fundierte Entscheidungen über die Eignung oder Nichteignung biometrischer Systeme zu treffen. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden können ihr Wissen und ihre Lösungskompetenzen in einer Vielzahl unerwarteter Situationen anwenden. Ausdruck dessen ist z.B. die

	Fähigkeit, die Erkennungsgenauigkeit, Sicherheit und Flexibilität biometrischer Lösungen durch Kombination verschiedener Biometrien auf unterschiedlichen Ebenen mittels verschiedener Fusionierungsstrategien zu verbessern. <u>Kooperation und Kommunikation</u> Die Studierenden gewährleisten durch konstruktives, konzeptionelles Handeln die Durchführung von situationsadäquaten Lösungsprozessen. <u>Wissenschaftliche Selbstverständnis/ Professionalität</u> Die Studierenden entwickeln wissenschaftliche Professionalität, die sie in die Lage versetzt, ihre im Modul erworbenen Kenntnisse über das kritische Thema Sicherheit biometrischer Systeme kontinuierlich zu aktualisieren. Inhaltlicher Fokus liegt hier besonders auf den sich aktuell rasant entwickelnden Ansätzen zur Erkennung von Präsentationsattacken und sogenannten Privacy Enhancement Techniken, wie erneuerbaren Biometrietemplates.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbrief und Literatur. Ergänzend zum Lehrbuch werden wissenschaftliche Artikel und Veröffentlichungen bereitgestellt, um die Lehrbuchinhalte zu vertiefen, weiterführendes Selbststudium zu unterstützen und aktuellste Entwicklungen (z.B. Biometriestandards) abzudecken. Zusätzlich werden online eLearning Module und lauffähige Fingerabdruck-, Gesichts- und Iriserkennungssystemen bereitgestellt. Mit Hilfe dieser in VMs bereitgestellten Biometriesysteme werden komplexe praktische Projekte durchgeführt. 90-minütiges Webinar sowie Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen.
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik und Informatik
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	2. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Kryptoanalyse	
Modulbezeichnung Englisch: Cryptographic Analysis	
Modulverantwortliche(r)	Prof. Dr.-Ing. habil. Andreas Ahrens
Inhalte des Moduls	• Methoden und Techniken, um Informationen aus verschlüsselten Texten zu gewinnen (Algebraische Angriffsmethoden, Lineare Kryptoanalyse, Brute-Force-Methode, Wörterbuchangriff, Man-in-the-middle-Angriff, Korrelationsattacken auf Stromchiffren und Algorithmen zum Lösen des Faktorisierungsproblems und des diskreten Logarithmusproblems (zum Brechen asymmetrischer Verfahren)) • Methoden für das formale Beweisen der Sicherheit von Protokollen, wie beispielsweise simulationsbasierte Beweise. Diese sollen an gängigen Protokollen wie Zero-Knowledge-Beweisen, Commitment-Schemes, oder Schlüsselvereinbarungsprotokollen illustriert werden.
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls die Fähigkeit, IT-Sicherheit präzise zu modellieren und zu analysieren. Sie sind mit kryptologischen Standard-Techniken auf einem hohen Niveau vertraut und können diese Techniken praktisch anwenden. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden sind befähigt, kryptografische Systeme und Angriffe bzgl. der Standard-Techniken zu analysieren. Die Studierenden besitzen die Fähigkeit, mathematische Kenntnisse flexibel zur Analyse und praktischen Durchführung von kryptografischen Verfahren anzuwenden. Sie sind in der Lage, kryptoanalytische Forschungsmethoden auszuwählen, diese zu begründen und die Ergebnisse kritisch zu diskutieren. <u>Kommunikation und Kooperation</u> Die Studierenden gewährleisten durch konstruktives, konzeptionelles Handeln die Durchführung von situationsadäquaten Lösungsprozessen. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden entwickeln wissenschaftliche Professionalität, die sie in die Lage versetzt, ihre im Modul erworbenen Kenntnisse über das Thema Kryptoanalyse kontinuierlich zu aktualisieren.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's,

	Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen; diverse Online-Projekte
Voraussetzung für die Teilnahme	Kenntnisse der modernen Kryptografie
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	2. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Sicherheit im Cloud-Computing	
Modulbezeichnung Englisch: Security in Cloud-Computing	
Modulverantwortliche(r)	Prof. Dr.-Ing. Meiko Jensen

Inhalte des Moduls	• Grundlagen des Cloud-Computing:
	  o Geschäftsmodelle
	  o Dienstmodelle
	  o Technische Grundlagen
	• Sicherheit für Cloud-Computing
	  o Virtualisierungs-Sicherheit
	  o Sicherheit von Web-Anwendungen
	  o Service-Level Agreements
	  o Datenschutz-Anforderungen
	• Sichere Datenspeicherung

Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls Kenntnisse über die technischen und wirtschaftlichen Grundlagen des Cloud-Computings sowie die besonderen Sicherheitsanforderungen dieser Architektur. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden sind in der Lage, passende Sicherheitslösungen auf konkrete und komplexe Einsatzszenarien zu analysieren, zu vergleichen und zu bewerten. Sie können dazu aktuelle wissenschaftliche Literatur auswerten, zusammenfassen und präsentieren. Die Studierenden kennen die Informationsquellen zum Thema Cloud-Computing, die sie für ihre Weiterbildung nutzen können. <u>Kommunikation und Kooperation</u> Die Studierenden sind befähigt, selbstständig wissenschaftliche Literatur zum Thema Cloud-Computing zu recherchieren und sich darüber mit den Kommilitonen auszutauschen. Sie erkennen Konfliktpotentiale in der Zusammenarbeit mit anderen und reflektieren diese vor dem Hintergrund situationsübergreifender Bedingungen. Sie binden Beteiligte unter der Berücksichtigung der jeweiligen Gruppensituation zielorientiert in Aufgabenstellungen ein. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden sind in der Lage, sich an Zielen und Standards professionellen Handelns in Bezug auf die Kooperation in einer Gruppe sowohl in der Wissenschaft als auch den Berufsfeldern außerhalb der Wissenschaft zu orientieren. Sie können erarbeitetes Wissen in der Gruppe evaluieren und erkennen situationsadäquat und situationsübergreifend Rahmenbedingungen ihres Handelns.

ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und aktueller wissenschaftlicher Literatur; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik und Informatik, im Netzwerk- und Sicherheitsmanagement
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	2. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Forensik in Betriebs- und Anwendungssystemen	
Modulbezeichnung Englisch: Digital Forensic Science in Operating and Software Systems	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	• Vermittlung von detailliertem Wissen über Teilgebiete der IT-Forensik: Datenträger-, Live-, Betriebssystem-, Netzwerk-, Mobile, Big Data-, Browser-Forensik, Forensik in IT-Anwendungen, u.a. • Übersicht über die Quellen forensischer Daten • Übersicht über die Vorgehensweise bei der Sicherung von forensischen Daten • Forensische Daten in Betriebssysteme Windows, LINUX, Android, iOS o Konfigurationsdaten o Hardware-, Prozess- und Sitzungsdaten o Kommunikationsprotokolldaten o Logdaten • Forensik in Filesystemen o Dateisystem FAT, NTFS, EXTx (Struktur, Verwaltung, Datenablage, Sicherheit) • Übersicht über Netzwerk- und Cloud-Forensik • Übersicht über Möglichkeiten der forensischen Analyse (LOG-Files, Verlaufsdaten, etc.) in verschiedenen IT-Anwendungen anhand von Beispiel-Anwendungen (z.B. Browser, Soziale Medien, Office-Anwendungen, SAP, u.a.) • Techniken zum Auslesen von forensischen Daten in relationalen und NoSQL -Datenbanken • Techniken zur Big Data-Analyse • Gruppen-Projekt zu einem ausgewählten Themen-bereich, schriftliche und mündliche Präsentation
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls detailliertes Wissen über die Teilgebiete der IT-Forensik. Sie kennen die Probleme und Vorgehensweisen in den einzelnen IT-Forensik-Teilgebieten, können Vorfälle einordnen und gerichtsverwertbar eine IT-forensische Analyse initiieren. Sie besitzen auf einem der Teilgebiete detaillierte Kenntnisse und vertiefte Fähigkeiten. Sie kennen die für diesen Teilbereich verfügbaren Analysemöglichkeiten bzw. Tools und können diese bewerten. Sie sind in der Lage, komplexe IT-Forensik-Szenarien zu analysieren und Teilaufgaben zu separieren. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden sind in der Lage, Sicherheitslösungen und komplexe IT-Systeme auf konkrete IT-Forensik-Analyseszenarien zu analysieren, zu vergleichen und zu bewerten. Sie können dazu aktuelle wissenschaftliche

	Literatur auswerten, zusammenfassen und präsentieren. Sie sind in der Lage, Forschungsfragen zu dieser Thematik zu entwerfen und wählen konkrete Wege der Operationalisierung zu einer Forschungsfrage aus und können diese auch schriftlich begründen. Die Studierenden verteidigen diese Ergebnisse und interpretieren diese kritisch. Die Studierenden kennen die Informationsquellen zum Thema IT-Forensik, haben praktische Erfahrungen gesammelt und nutzen diese für ihre Weiterbildung. <u>Kommunikation und Kooperation</u> Die Studierenden sind befähigt, selbstständig wissenschaftliche Literatur zu recherchieren, sich darüber mit den Kommilitonen auszutauschen und eine gemeinsame Präsentation zu erarbeiten. Sie erkennen Konfliktpotentiale in der Zusammenarbeit mit anderen und reflektieren diese vor dem Hintergrund situationsübergreifender Bedingungen. Sie binden Beteiligte unter der Berücksichtigung der jeweiligen Gruppensituation zielorientiert in Aufgabenstellungen ein. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden sind in der Lage, sich an Zielen und Standards professionellen Handelns in Bezug auf die Kooperation in einer Gruppe sowohl in der Wissenschaft als auch den Berufsfeldern außerhalb der Wissenschaft zu orientieren. Sie können erarbeitetes Wissen in der Gruppe evaluieren und erkennen situationsadäquat und situations-übergreifend Rahmenbedingungen ihres Handelns.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen; diverse online-Projekte
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik, Informatik, IT-Sicherheit und der IT-Forensik
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung und 90-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	2. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Compliance Manager Datenschutz	
Modulbezeichnung Englisch: Compliance Manager Privacy	
Modulverantwortliche(r)	Karsten Neumann
Inhalte des Moduls	• materielles Datenschutzrecht im nicht-öffentlichen Bereich: die Befugnisnormen des BDSG/EuDSGVO • materielles Datenschutzrecht im öffentlichen Bereich: die Befugnisnormen im BDSG/LandesDSG • formelles Datenschutzrecht: Genehmigungen, Betroffenen-Rechte, Dokumentation der Verfahren, Durchführung von Audits, Prüfung von Auftragsdatenverarbeitern, Vorabkontrolle von Verfahren, Risikobewertungen • Datenschutz als Managementaufgabe: die Organisation und Steuerung der Datenschutz-Compliance-Prozesse im Unternehmen • Arbeit als Datenschutzbeauftragte
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls Kenntnisse über datenschutzrechtliche Befugnisnormen in den wichtigsten Bereichen der betrieblichen Praxis (Kundendatenverarbeitung, Marketing, Mitarbeiterdatenverarbeitung, Zulässigkeit der Datenübermittlung in Drittstaaten, Auftragsdatenverarbeitung) Die Studierenden kennen die europarechtlichen und internationalen Rahmenbedingungen, die Datenverarbeitung im internationalen Konzern, das Datenschutzrecht in der aufsichtsbehördlichen Praxis, sowie das Datenschutzrecht im rechtlichen Umfeld zu Wettbewerbs- und Verbraucherschutzrecht. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden sind befähigt, selbstständig und sicher datenschutzrechtliche Befugnisnormen in den wichtigsten Bereichen der behördlichen Praxis nach Bundes- und Landesdatenschutzrecht anzuwenden. Des Weiteren sind die Studierenden zur Organisation und Steuerung der datenschutzrechtlich erforderlichen innerbetrieblichen Prozesse (Sicherstellung einer ordnungsgemäßen Datenverarbeitung, Angemessenheit der technisch-organisatorischen Maßnahmen, Wahrung der Betroffenenrechte, revisionssichere Dokumentation der Verfahren, Schulung der Mitarbeiter, Überwachung der Auftragsdatenverarbeiter, Zusammenarbeit mit den Aufsichtsbehörden) befähigt. <u>Kooperation und Kommunikation</u> Die Studierenden haben ihre fachübergreifende (Informatik-Recht) Kommunikationskultur weiterentwickelt. Sie sind in

	der Lage, technische und juristische Aspekte in Diskussionen zur IT-Sicherheit sicher einzubringen und die unterschiedlichen Sichtweisen in Diskussionen zu respektieren. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden haben hinsichtlich der Thematik des Datenschutzes ihre Befähigung ausgebaut, ihr berufliches Handeln in Bezug auf gesellschaftliche Erwartungen und Folgen zu reflektieren und entwickeln ihr berufliches Handeln entsprechend weiter.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	2. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Industrial Security	
Modulbezeichnung Englisch: Industrial Security	
Modulverantwortliche(r)	Prof. Dr. Nils Gruschka
Inhalte des Moduls	• IT-Sicherheitskonzepte für Industrie 4.0-Anwendungen • Grundlagen: o Automatisierung o Geschäftsmodelle o Cyber-physikalische Systeme o Internet of Things o M2M-Kommunikation • Angriffe und Gefahren • Sicherheit: o Physikalische Sicherheit o Netzwerkschutz o Malware-Abwehr o M2M-Sicherheit o Datensicherheit
Qualifikationsziele des Moduls	Wissen und Verstehen Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls Kenntnisse über die Grundlagen und des aktuellen Standes der Technik der industriellen Automatisierung. Sie wägen die fachliche erkenntnistheoretisch begründete Richtigkeit von Strategien und Vorgehensweisen zur industriellen Automatisierung unter Einbezug wissenschaftlicher und methodischer Überlegungen gegeneinander ab und können unter Zuhilfenahme dieser Abwägungen praxisrelevante, komplexe und wissenschaftliche Probleme lösen. Einsatz, Anwendung und Erzeugung weiterführenden Wissens Die Studierenden sind in der Lage Sicherheitsprobleme, die sich in diesem Kontext ergeben, zu analysieren und zu bewerten. Des Weiteren sind sie mit diesem weiter über das Bachelorniveau hinausgehenden Wissen befähigt, mögliche Strategien zu erarbeiten, um die Sicherheit solcher Systeme zu erhalten bzw. zu erhöhen. Sie sind in der Lage, Forschungsfragen zu dieser Thematik zu entwerfen und wählen konkrete Wege der Operationalisierung zu einer Forschungsfrage aus und können diese auch schriftlich begründen. Sie erläutern Forschungsergebnisse und interpretieren diese kritisch. Kommunikation und Kooperation Die Studierenden sind befähigt, selbstständig wissenschaftliche Literatur zu recherchieren, sich darüber mit den Kommilitonen auszutauschen und eine gemeinsame Präsentation zu erarbeiten. Sie erkennen Konfliktpotentiale in der Zusammenarbeit mit anderen und reflektieren diese

	vor dem Hintergrund situationsübergreifender Bedingungen. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden haben ihre Fähigkeiten vertieft, sich an Zielen und Standards professionellen Handelns in Bezug auf die Kooperation in einer Gruppe sowohl in der Wissenschaft als auch den Berufsfeldern außerhalb der Wissenschaft zu orientieren. Sie können erarbeitetes Wissen in der Gruppe evaluieren und erkennen situationsadäquat und situationsübergreifend Rahmenbedingungen ihres Handelns.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und wissenschaftlicher Literatur; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik, Informatik
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung: Präsentation und schriftliche Ausarbeitung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	3. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Systemanalyse und Systemhärtung	
Modulbezeichnung Englisch: Systems Analysis Methods for Digital Forensic Data	
Modulverantwortliche(r)	Prof. Dr. Olaf Hagendorf
Inhalte des Moduls	• IT-Sicherheit und Sicherheitsmaßnahmen • Motivation und Schwachstellen von vernetzten Rechnersystemen, • Verfahren und Mechanismen zur Systemanalyse • Tools zur Systemanalyse • Verfahren und Mechanismen zur Systemhärtung • Tools zur Systemhärtung • Paketfilter, Circuit- und Application-Level Gateways • Intrusion Detection und Prevention-Systeme zur Angriffserkennung und -abwehr • Logfileanalyse und Analyse von Webaktivitäten
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden verfügen nach erfolgreichem Abschluss des Moduls über ein breites, detailliertes und kritisches Verständnis auf dem neuesten Stand des Wissens über die Analyse von Rechnern und Netzwerkkomponenten in vernetzten Systemen sowie über die Sammlung von Systeminformationen und über Tools zur Systemanalyse. Die Studierenden wägen die fachlich erkenntnistheoretisch begründete Richtigkeit unter Einbezug wissenschaftlicher und methodischer Überlegungen gegeneinander ab und können unter Zuhilfenahme dieser Abwägungen praxisrelevante, komplexe und wissenschaftliche Probleme lösen. <u>Einsatz, Anwendung und Erzeugung von Wissen</u> Die Studierenden kennen die Mechanismen und Strategien zur Erhöhung der Sicherheit von Rechnern und können diese anwenden und bewerten. Sie sind des Weiteren befähigt, auch Tools zur Systemhärtung und zur Logfileanalyse anzuwenden und zu bewerten. Die Studierenden können neues Wissen in vorhandenes Wissen integrieren und dieses auf komplexe Zusammenhänge (z.B. Fallstudien zur Systemhärtung) anwenden. Sie erläutern Forschungsergebnisse und interpretieren diese kritisch. Sie sind in der Lage, sich selbstständig neues Wissen und Können auf dem Gebiet der Systemhärtung anzueignen. <u>Kommunikation und Kooperation</u> Die Studierenden gewährleisten durch konstruktives, konzeptionelles Handeln die Durchführung von situationsadäquaten Lösungsprozessen.

	<u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden entwickeln wissenschaftliche Professionalität, die sie in die Lage versetzt, ihre im Modul erworbenen Kenntnisse über das Thema Systemhärtung kontinuierlich zu aktualisieren.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD bzw. Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen; Online-Projekte
Voraussetzung für die Teilnahme	Grundkenntnisse in Informatik, Mathematik, Betriebssysteme, Netzwerk- und Sicherheitsmanagement, IT-Forensik
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	3. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Analysemethoden für forensische Daten	
Modulbezeichnung Englisch: Analysis Methods for Digital Forensic Data	
Modulverantwortliche(r)	Dipl.-Ing. Hans-Peter Merkel
Inhalte des Moduls	• Vorgehensweise bei einer IT-Forensischen Untersuchung • Identifizierung und Datensicherung von relevanten Datenquellen • Wiederherstellung von gelöschten und geänderten Daten • Umgang mit Verschlüsselung • Dateianalyse: Allocated, Unallocated, Carving • Einsatz der Virtualisierung in der Forensik • Parallelen und Gemeinsamkeiten der Forensik zu mobilen Geräten • Kennenlernen von IT-Forensik-Werkzeugen auf Linux-Basis • Zeitstempel Informationen einbinden (Timelines und Supertimelines) • Windows spezifische Artefakte (VSS, Prefetch, Registry) • Durchführung von Beispiel-Auswertungen und Verfassen eines IT-Forensischen Berichtes • Individuelles IT-Forensik-Projekt mit einem praktischen komplexen Beispiel
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls die Fähigkeit, die Möglichkeiten und die Erfolgsaussichten einer IT-forensischen Analyse mittels Linux-basierenden Werkzeugen abzuschätzen. Sie verfügen über ein breites, detailliertes und kritisches Verständnis auf dem neuesten Stand des Wissens über komplexe Anwendungsszenarien, Maßnahmen und Tools. Die Studierenden besitzen Kenntnisse darüber, wie die forensisch erfassten Daten als Beweismittel in Form eines Reports gerichtsverwertbar zu sichern und zu dokumentieren sind. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden sind in der Lage IT-Forensik-Probleme, detailliert auf Basis von frei verfügbaren Linux-Werkzeugen zu analysieren und zu bewerten. Des Weiteren sind sie mit diesem weiter über das Bachelorniveau hinausgehenden Wissen befähigt, mögliche Strategien zu erarbeiten, um die IT-Forensische Fragestellungen wissenschaftlich fundiert kreativ zu bearbeiten und zu lösen. Die Studierenden können die Einsatzmöglichkeiten von Linux-Werkzeugen und kommerziellen Windows-Werkzeugen abwägen. Sie sind in der Lage, Forschungsfragen auf dem Gebiet der IT-Forensik

	zu entwerfen, wählen konkrete Wege der Operationalisierung einer Forschungsfrage aus, müssen diese verteidigen und auch kritisch diskutieren. Sie sind in der Lage, selbständig einen technischen forensischen Bericht zu verfassen. <u>Kommunikation und Kooperation</u> Die Studierenden sind befähigt, selbstständig wissenschaftliche Literatur zu recherchieren, sich darüber mit den Kommilitonen auszutauschen und selbständig einen schriftlichen Bericht zu erarbeiten. Sie erkennen die technischen Rahmenbedingungen eines IT-Forensischen Berichtes und können diese anwenden. <u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden haben ihre Fähigkeiten vertieft, sich an Zielen und Standards in Bezug auf die professionelle Aufarbeitung einer IT-Forensischen Problemstellung zu orientieren. Sie sind in der Lage, das eigene berufliche Handeln auf dem Gebiet der IT-Forensik mit theoretischem und methodischem Wissen zu begründen und reflektieren es hinsichtlich alternativer Entwürfe. Sie haben ihr berufliches Selbstverständnis geschärft, in dem sie sich mit dem Einsatz von frei verfügbare Linux-Werkzeugen vs. dem Einsatz von kommerziellen Windows-Werkzeuge vs. dem Einsatz von wissenschaftlichen Methoden beschäftigt haben.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und wissenschaftliche Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen; online-Modul zur praktischen Abarbeitung von IT-Forensischen Analysen
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik, Informatik, Betriebssysteme, Netzwerke, IT-Forensik
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung: IT-Forensischer Bericht bzgl. der Auswertung eines Beispielszenarios
Arbeitsaufwand	125 h davon 8 h seminaristischer Unterricht
Leistungspunkte	5 CP
Angebotsturnus	3. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Kriminalpsychologie	
Modulbezeichnung Englisch: Criminal Psychology	
Modulverantwortliche(r)	Dipl. Kriminalist Uwe Rüffer
Inhalte des Moduls	• Wenn der Blick auf Bits und Bytes nicht genügt – Einführung in das Fachgebiet, Psychologische Grundlagen für die Erklärung menschlichen Verhaltens • Die Systembestandteile des Menschen - Was unsere Auffassung von Wirklichkeit beeinflusst • Was zwischen 1 und 0 liegt – Gütekriterien der Information • Ein psychologischer Blick auf Datenein- und -ausgabe - Gesprächsführung • Die internen (menschlichen) Datenverarbeitungsprozesse – kriminalistisches Denken im Untersuchungsprozess • Mögliche Fehler im (menschlichen) Kern – Kriminalpsychologische Aspekte
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls ein Verständnis sowie Kenntnisse über die psychologischen Grundlagen für menschliches Verhalten, deren Entwicklung und Anwendung auf forensische Untersuchungsprozesse. Das schließt die Kenntnis des dazugehörigen Fachvokabulars mit ein. Des Weiteren haben sie Vorstellungen zu Wahrnehmungs- und Gedächtnisprozessen, Emotionen und Motivationen sowie deren mögliche Auswirkungen auf Untersuchungs- und Beurteilungsverhalten. Den Studierenden werden zu einer kriminalistisch-psychologischen und kriminalpsychologischen Betrachtung der IT-Kriminalität angehalten. Sie haben Wissen zu kriminalpsychologischen und forensisch psychologischen Aspekten der Untersuchung von IT-Kriminalität. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden sind in der Lage, ihre Wahrnehmungen und Beurteilungen zu relativieren, Informationen in Ihrer Güte zu beurteilen, Versionen zu Motiven kriminellen Verhaltens zu bilden. Sie können IT-sicherheitskritische Vorfälle kriminalpsychologisch einordnen. <u>Kooperation und Kommunikation</u> Die Studierenden haben eine fachübergreifende (Informatik-Psychologie) Kommunikationskultur entwickelt. Sie sind in der Lage, technische und psychologische Aspekte in Diskussionen zur IT-Sicherheit einzubringen und die unterschiedlichen Sichtweisen in Diskussionen zu respektieren.

	<u>Wissenschaftliches Selbstverständnis/ Professionalität</u> Die Studierenden sind befähigt, ihr berufliches kriminalpsychologisches Handeln in Bezug auf gesellschaftliche Erwartungen und Folgen zu reflektieren und entwickeln ihr berufliches Handeln entsprechend weiter.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur; 90-minütiges Webinar und Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	100 h davon 8 h seminaristischer Unterricht
Leistungspunkte	4 CP
Angebotsturnus	3. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Ethische Probleme der Informationstechnologie	
Modulbezeichnung Englisch: Ethical Aspects in Information Technology	
Modulverantwortliche(r)	Dr. phil. Roland Reiske
Inhalte des Moduls	Das Modul führt grundlegend in die Ethik und ihre Problemstellungen ein. Es werden Kenntnisse über die Struktur ethischer Probleme und Dilemmata vermittelt und Entscheidungskriterien zu ihrer Lösung erarbeitet. Darauf aufbauend werden anwendungsbezogene Probleme der praktischen Ethik betrachtet, die sich insbesondere auf Informationstechnologien beziehen, insbesondere auf die die Erhebung, Speicherung, Übermittlung, Verarbeitung und Nutzung von Daten und auf Technologien, die darauf beruhen – bspw. Künstliche Intelligenzen (KI). Das Ziel ist die Schaffung bzw. Schärfung eines Problembewusstseins für ethische Fragestellungen.
Qualifikationsziele des Moduls	Wissen und Verstehen Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls grundlegende Kenntnisse über ethische Grundpositionen und kennen das ethische Fachvokabular. Einsatz, Anwendung und Erzeugung weiterführenden Wissens Die Studierenden sind in der Lage, ethische Konflikte zu erkennen, zu bewerten und einer ethisch vertretbaren Problemlösung zuzuführen. Sie können IT-sicherheitskritische Vorfälle ethisch einordnen. Kooperation und Kommunikation Die Studierenden haben eine fachübergreifende (Informatik-Ethik) Kommunikationskultur entwickelt. Sie sind in der Lage, technische und ethische Aspekte in Diskussionen zur IT-Sicherheit einzubringen und die unterschiedlichen Sichtweisen in Diskussionen zu respektieren. Wissenschaftliches Selbstverständnis/ Professionalität Die Studierenden sind befähigt, ihr berufliches Handeln in Bezug auf gesellschaftliche Erwartungen und Folgen ethisch zu reflektieren und entwickeln ihr berufliches Handeln entsprechend weiter. Das Bewusstsein für die Notwendigkeit ethischer Normen und der Ausrichtung menschlicher Handlungen an ihnen wird bei den Studierenden geschärft.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen

Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Arbeitsaufwand	100 h davon 8 h seminaristischer Unterricht
Leistungspunkte	4 CP
Angebotsturnus	3. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Masterseminar	
Modulbezeichnung Englisch: Master's Seminar	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	• Selbständige Erarbeitung der Regeln zum wissenschaftlichen Arbeiten mittels des eLearning-Moduls • Wahl und Ausarbeitung eines Themas • Diskussion über die Inhalte des Themas mit den Betreuern • Ausarbeitung eines Exposés zum geplanten Master Thesis Thema • Vorträge durch die Master-Kandidaten über die für die Master Thesis gewählte Problemstellung • Qualifiziertes Feedback durch den Dozenten und die Studenten
Qualifikationsziele des Moduls	Wissen und Verstehen Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls Kenntnisse über die Regeln für die Erstellung von wissenschaftlichen Arbeiten in Vorbereitung auf die Master Thesis. Einsatz, Anwendung und Erzeugung weiterführenden Wissens Die Studierenden haben vertiefte Kenntnisse und Fähigkeiten, eigenständig eine Problemstellung aus einem Forschungsgebiet auszuwählen, sich mit diesem Forschungsgebiet detaillierter auseinanderzusetzen und eine wissenschaftliche Problem- und Literaturrecherche durchzuführen. Sie sind in der Lage, ihre Problemstellung mit anderen technisch und rechtlich zu diskutieren und die Ergebnisse in einer schriftlichen, wissenschaftlichen Ausarbeitung (Exposé) zusammenzufassen. Sie sind weiterhin in der Lage, die Ausarbeitung in einem kurzen Vortrag zu präsentieren. Kooperation und Kommunikation Die Studierenden haben eine Kommunikationskultur etabliert und weiterentwickelt, die sie zur Lösung von Problemstellungen einsetzen. Sie tauschen sich sach- und fachbezogen mit Vertreterinnen und Vertretern unterschiedlicher akademischer und nicht-akademischer Handlungsfelder über alternative, theoretisch begründbare Problemlösungen aus.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung und 90-minütiges Webinar zur

	Prüfungsvorbereitung und Klärung offener Fragen; eLearning-Modul zum wissenschaftlichen Arbeiten
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung: Exposé und 15min-Vortrag zum geplanten Thema der Master Thesis
Arbeitsaufwand	50 h davon 8 h seminaristischer Unterricht
Leistungspunkte	2 CP
Angebotsturnus	3. Semester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben.

Modulbezeichnung Deutsch: Master Thesis	
Modulbezeichnung Englisch: Master's Thesis	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	Es handelt sich um eine praxisbezogene theoretische Auseinandersetzung mit aktuellen und/oder wissenschaftliche Fragestellungen aus einem Teilgebiet des Studiums. Die Thesis sollte inhaltlich anspruchsvoll, wissenschaftlich theoretisch fundiert und zugleich praxisbezogen ausgerichtet sein. Mit Hilfe der Analyse und Auswertung aktueller Erkenntnisse des Fachgebietes, sollen die Studierenden auf der Basis ihres Wissens eigene Standpunkte aufstellen, Lösungsansätze entwickeln und diese in geeigneter Weise darstellen. Wesentlicher Inhalt des Kolloquiums ist die mündliche Präsentation der Inhalte und Ergebnisse der vorangegangenen Thesis der Studierenden. Im Anschluss an die mündliche Präsentation erfolgt eine Diskussion über eventuelle Unklarheiten oder Schwachstellen der Thesis sowie über themenübergreifende, das Studium betreffende Inhalte.
Qualifikationsziele des Moduls	Der Anspruch eines Studiums ist es, neben der fachspezifischen Vermittlung von berufspraktischen Inhalten, Studierende zur selbstständigen wissenschaftlichen und interdisziplinären Recherche und Problemanalyse zu befähigen. Im Rahmen einer Thesis soll dokumentiert werden, dass die Studierenden in der Lage sind, innerhalb einer vorgegebenen Frist ein fachspezifisches Problem selbstständig mit dem im Studium erlernten Fach- und Methodenwissen nach wissenschaftlichen Methoden zu bearbeiten sowie einen Themenbereich vertieft analysieren und weiterentwickeln zu können und gewonnene Ergebnisse in die wissenschaftliche und fachpraktische Diskussion einzuordnen. Die Thesis wird durch das Kolloquium ergänzt. Im Rahmen des Kolloquiums soll festgestellt werden, ob die Studierenden in der Lage sind, die Ergebnisse ihrer Thesis in überzeugender Weise, unter Berücksichtigung der fachlichen Grundlagen und interdisziplinären Zusammenhänge, mündlich zu präsentieren und selbstständig zu begründen sowie ggf. die Bedeutung für die Praxis mit einzubeziehen. Ebenso erhalten die Studierenden die Möglichkeit auf eventuelle Unklarheiten und Schwachstellen ihrer Thesis einzugehen und diese richtig zu stellen.

	Themenfindung der Thesis erfolgt in Absprache mit dem Betreuer unter Berücksichtigung folgender Punkte: • Einordnung in den Studiengang • Umfang • wissenschaftlicher Anspruch • Praxisrelevanz • ausreichendes Vorhandensein entsprechender Literatur Das Kolloquium behandelt das Thema der jeweiligen Thesis der Studierenden sowie angrenzende, das Studium betreffende Inhalte.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Bei der Master Thesis handelt es sich um die eigenständige, durch Beratung unterstützte, individuelle Verfassung einer wissenschaftlichen Abschlussarbeit. Das Kolloquium (– mündliche Präsentation und Verteidigung der Inhalte der Thesis) findet in Form einer hochschulöffentlichen Veranstaltung statt, sofern der/ die Studierende nicht widerspricht bzw. das jeweilige Thema unter Ausschluss der Öffentlichkeit behandelt werden muss.
Voraussetzung für die Teilnahme	Das Thema der Thesis wird ausgegeben, wenn Credits gemäß Prüfungsordnung nachgewiesen werden können. Voraussetzung für die Teilnahme am Kolloquium ist das erfolgreiche Einreichen der Thesis.
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Wiss. Arbeit (Master-Thesis) und 45 min. Kolloquiums (30 min. Präsentation und 15 min. Diskussion zum Bachelor-Thema)
Arbeitsaufwand	500h (499h 15 min. Selbststudium und 45 min. Kolloquium)
Leistungspunkte	20 CP
Angebotsturnus	4. Semester
Dauer des Moduls	1 Semester
Literaturangaben	wird entsprechend des Themas gewählt