Modulhandbuch
Master-Studiengang IT-Sicherheit und Forensik
Version 12.4.2018

Modul 1: Einführung in die IT-Sicherheit und Forensik

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Einführung in die IT-Sicherheit und Forensik
Kürzel	EF
Dauer des Moduls	1 Semester
Angebotsturnus	1. Semester
Modulverantwortliche(r)	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in)	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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; fakultative Projekte in der VM mit X-Ways, DBMS, etc.
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Grundkenntnisse in Mathematik und Informatik
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 -analyse. 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.

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 Bedrohungssituationen und Angriffsszenarien • 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.) • Vermittlung von Wissen über eine Datensammlung und Datenanalyse • Vermittlung von Wissen über eine Gerichtsverwertbare Dokumentation
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 Carrier, B.: File System Forensic Analysis. Addison-Wesley,2005 🕮 Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011 🕮 Geschonneck, A.: Computer Forensik. dpunkt Verlag, 6. Aufl., 2014 🕮 Leitfaden IT-Forensik, Version 1.0.1, März 2011, Bundesamt für Sicherheit in der Informationstechnik, Bonn 🕮 Kuhlee, L., Völzow, V.: Computer-Forensik Hacks. O'Reilly Verlag GmbH & CO. KG, Köln, 2012 🕮 Dewald A., Freiling, F. C.: Forensische Informatik, Books on demand, Norderstedt, 1. Aufl., August 2011 🕮 Ballmann, B.: Network Hacks, Springer Vieweg, 2012 🕮 Androulidakis: Mobile Phone Security and Forensics – A practical Approach, Springer Science and Business Media, New York, 2012 🕮 Hayes, D.R.: A Practical Guide to Computer Forensics Investigations, Pearson Education, Inc. Indianapolis, 2015 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 2: Netzwerk- und Sicherheitsmanagement

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Netzwerk- und Sicherheitsmanagement
Kürzel	NSM
Dauer des Moduls	1 Semester
Angebotsturnus	1. Semester
Modulverantwortliche(r)	Prof. Dr.-Ing. E. Jonas
Dozent(in)	Prof. Dr.-Ing. E. Jonas
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Lehr- und Lernform	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
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Grundkenntnisse in Informatik, Mathematik, Betriebssysteme, Kommunikationstechnik
Qualifikationsziele des Moduls	<u>Wissen und Verstehen</u> Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls vertiefte Kenntnisse über den Aufbau, die Struktur und die Funktionsweise von Rechnernetzen. Des Weiteren kennen sie die 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.

Inhalte des Moduls	• Motivation und OSI-Sicherheitsarchitektur, • Security Engineering: Vorgehensmodell, Sicherheitsprobleme, Bedrohungen • Sicherheitsmechanismen (Verschlüsselung, Integritätssicherung, Verfügbarkeit, Authentizität und Verbindlichkeit) • Komplexe Sicherheitsmechanismen (IPSec, SSL/TLS, SSH, VPN) • WLAN-Sicherheit • Netzwerkmanagement in Betriebssystemen
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 Claudia Eckert: IT-Sicherheit, Konzepte – Verfahren – Protokolle. 7. Überarbeitete und erweiterte Auflage, Oldenbourg-Verlag, 2012 🕮 Bernhard C. Witt: IT-Sicherheit kompakt und verständlich, 2. Auflage, Springer Verlag, 2018 🕮 Charles P. Pfleeger, Sharie L. Pfleeger: Security in Computing, Pearson 2006/2008 🕮 Simson Garfikel, Gene Spafford: Practical UNIX & Security, O'Reilly, 2003 🕮 Werner Prguntke: Basiswissen IT-Sicherheit, 3. Auflage, Springer Campus, 2017 🕮 Bruce Schneider: Angewandte Kryptographie, Pearson Studium, 2005 🕮 Martin Kappes: Netzwerk- und Datensicherheit, Eine praktische Einführung, Springer Vieweg, 2013 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 3: Kryptographische Methoden und Anwendungen

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Kryptographische Methoden und Anwendungen
Kürzel	KM
Dauer des Moduls	1 Semester
Angebotsturnus	1. Semester
Modulverantwortliche(r)	Prof. Dr.-Ing. habil. A. Ahrens
Dozent(in)	Prof. Dr.-Ing. habil. A. Ahrens
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Grundkenntnisse in Mathematik, Informatik und Programmierung
Qualifikationsziele des Moduls	Wissen und Verstehen Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls Kenntnisse über grundlegende Probleme der IT-Sicherheit und deren Zusammenhang zur Verschlüsselungsproblematik. Sie lernen wichtige kryptographische Verfahren und deren mathematische Grundlagen kennen. Sie sind in der Lage Besonderheiten, Grenzen, Terminologien und Lehrmeinungen des Lehrgebiets zu definieren und zu interpretieren. Einsatz, Anwendung und Erzeugung weiterführenden Wissens Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von symmetrischen 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 kryptographischen Verfahrungen zu treffen und reflektieren kritisch mögliche Folgen. Kommunikation und Kooperation Die Studierenden haben gelernt, sich sach- und fachbezogen untereinander über alternative, theoretisch begründbare Problemlösungen auszutauschen. Wissenschaftliches Selbstverständnis/ Professionalität Die Studierenden sind in der Lage, das eigene berufliche Handeln bzgl. des Einsatzes von kryptographischen 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.
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 • Kryptographische Anwendungen: Diffie-Hellman Schlüsselaustausch, ElGamal Verschlüsselung, DSA Signaturen
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 Beutelsbacher, A.; Schwenk,J.;Wolfenstetter, K.-D.: Moderne Verfahren der Kryptographie. Wiesbaden: Vieweg+Teubner, 2010 🕮 Beutelspacher, A.; Neumann, H.B.; Schwarzpaul, T.: Kryptografie in Theorie und Praxis. Wiesbaden: Vieweg+Teubner, 2009 🕮 Paar, C.; Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners.Berlin, Heidelberg: Springer, 2009. 🕮 Delfs, H., Knebl, H.:Introduction to Cryptography. Principles and Applications. Berlin, Heidelberg: Springer, 2002. 🕮 Mollin, R.A.: RSA and Public-Key Cryptography. Boca Raton, London, New York: CRC Press, 2003. 🕮 Stallings, W.: Cryptography and Network Security: Principles and Practice. Prentice Hall, 2010 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 4: Rechtliche Grundlagen der IT-Sicherheit und Forensik

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung:	Rechtliche Grundlagen der IT-Sicherheit und Forensik
Kürzel	RG
Dauer des Moduls	1 Semester
Angebotsturnus	1. Semester
Modulverantwortliche(r)	PD. Dr. iur. habil. M. Tamm
Dozent(in)	PD. Dr. iur. habil. M. Tamm
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	keine
Qualifikationsziele des Moduls	Wissen und Verstehen Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls die Befähigung zur Anwendung polizeilicher bzw. strafverfolgungsrechtlicher Handlungsbefugnisse im Grenzbereich zum Datenschutzrecht. Sie haben Wissen zu 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. Einsatz, Anwendung und Erzeugung weiterführenden Wissens Die Studierenden können IT-sicherheitskritische Vorfälle juristisch einordnen und juristische Aspekte in forensische Berichte integrieren. Sie sind befähigt, ausgewähltes juristisches Fachvokabular adäquat einzusetzen. Kooperation und Kommunikation 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. Wissenschaftliches Selbstverständnis/ Professionalität Die Studierenden sind befähigt, ihr berufliches Handeln in Bezug auf gesellschaftliche Erwartungen und Folgen zu reflektieren und entwickeln ihr berufliches Handeln entsprechend weiter.
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
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 Simitis, Siros: Bundesdatenschutzgesetz (Kommentar), 8. Aufl., Nomos, Baden-Baden 2014 🕮 Gohla, Peter/Schomerus, Rudolf (Hsrg.), BDSG: Bundesdatenschutzgesetz (Kommentar), 11. Aufl. Beck, München 2012 🕮 Däubler, Wolfgang: Kompaktkommentar zum BDSG, 4. Aufl., Bund Verlag, Frankfurt/M. 2011 🕮 Kühling, Jürgen, Datenschutzrecht, 2. Aufl., C.F. Müller, Heidelberg 2011 🕮 Leupold, Andreas/Glosser, Silke: Münchner Anwaltshandbuch IT-Recht, Beck 2011

Modul 5: Angewandte biometrische Systeme

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Angewandte biometrische Systeme
Kürzel	ABS
Dauer des Moduls	1 Semester
Angebotsturnus	2. Semester
Modulverantwortlicher	Prof. Dr.-Ing. Matthias Kreuseler
Dozent(in)	Prof. Dr.-Ing. Matthias Kreuseler
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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.
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CP
Voraussetzungen für die Teilnahme	Grundkenntnisse in Mathematik und Informatik
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 Modulteilnehmer 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 Biometriemplates.
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- o. Iriserkennung aus der Bewegung heraus
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 A. Jain, A.A. Ross, K. Nandakumar. Introduction to Biometrics. Springer 2011 🕮 M. Behrens, R. Roth. Biometrische Identifikation. Vieweg+Teubner Verlag, 2013. 🕮 V. Nolde, L. Leger. Biometrische Verfahren. Verlag Deutscher Wirtschaftsdienst 2008. 🕮 D. Maltoni, D. Maio, A. Jain, S. Prabhakar. Handbook of Fingerprint Recognition. Springer, 2009. 🕮 Behrens, M./Roth, R. (Hrsg.), Biometrische Identifikation, Grundlagen, Verfahren, Perspektiven, Vieweg DuD-Fachbeiträge 2001, ISBN 3-528-05786-6 🕮 Stan Z. Li, Anil K. Jain. Handbook of Face Recognition. Springer, 2005.

Modul 6: Kryptoanalyse

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Kryptoanalyse
Kürzel	KA
Dauer des Moduls	1 Semester
Angebotsturnus	2. Semester
Modulverantwortliche(r)	Prof. Dr.-Ing. habil. A. Ahrens
Dozent(in)	Prof. Dr.-Ing. habil. A. Ahrens
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Kenntnisse der modernen Kryptographie
Qualifikationsziele des Moduls	Wissen und Verstehen 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. Einsatz, Anwendung und Erzeugung weiterführenden Wissens Die Studierenden sind befähigt, kryptographische 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. Kommunikation und Kooperation Die Studierenden gewährleisten durch konstruktives, konzeptionelles Handeln die Durchführung von situationsadäquaten Lösungsprozessen. Wissenschaftliches Selbstverständnis/ Professionalität Die Studierenden entwickeln wissenschaftliche Professionalität, die sie in die Lage versetzt, ihre im Modul erworbenen Kenntnisse über das Thema Kryptoanalyse kontinuierlich zu aktualisieren.
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.
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 Beutelspacher, A.; Neumann, H.; Schwarzpaul, T. Kryptopgrafie in Theorie und Praxis. Wiesbaden: Vieweg+Teubner, 2010 🕮 Paar, C.; Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners.Berlin, Heidelberg: Springer, 2009. 🕮 Stallings, W.: Cryptography and Network Security: Principles and Practice. Prentice Hall, 2010 🕮 Brands, G.: Verschlüsselungsalgorithmen (Angewandte Zahlentheorie rund um Sicherheitsprotokolle), Wiesbaden: Vieweg+Teubner, 2002 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 7: Sicherheit im Cloud Computing

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Sicherheit im Cloud Computing
Kürzel	SCC
Dauer des Moduls	1 Semester
Angebotsturnus	2. Semester
Modulverantwortliche(r)	Prof. Dr. Nils Gruschka (FH Kiel)
Dozent(in)	Prof. Dr. Nils Gruschka (FH Kiel)
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	Selbststudium anhand von Lehrbriefen und aktueller *wissenschaftlicher* Literatur; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Grundkenntnisse in Mathematik und Informatik, im Netzwerk- und Sicherheitsmanagement
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, 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 situationsübergreifend Rahmenbedingungen ihres Handelns.
Inhalte des Moduls	• Grundlagen des Cloud Computing: o Geschäftsmodelle o Dienstmodelle o Technische Grundlagen o Service-orientierte Architekturen o Big Data • Sicherheit für Cloud Computing o Virtualisierungs-Sicherheit o Sicherheit von Web-Anwendungen o Datenschutz-Anforderungen o Sichere Datenspeicherung o Web-Service-Sicherheit
Voraussetzungen für die Vergabe von Leistungspunkten	Präsentation (25%) und 90-minütige schriftliche Prüfung (75%)
Literaturangaben	🕮 Gottfried Vossen, Till Haselmann, Thomas Hoeren: Cloud-Computing für Unternehmen: Technische, wirtschaftliche, rechtliche und organisatorische Aspekte, 2012 🕮 Udo Bub, Klaus-Dieter Wolfenstetter: Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing, 2014

Modul 8: Forensik in Betriebs- und Anwendungssystemen

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Forensik in Betriebs- und Anwendungssystemen
Kürzel:	FBA
Dauer des Moduls	1 Semester
Angebotsturnus	2. Semester
Modulverantwortliche(r)	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in)	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul
Lehr- und Lernform	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
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Grundkenntnisse in Mathematik, Informatik, IT-Sicherheit und der IT-Forensik
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 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 situationsübergreifend Rahmenbedingungen ihres Handelns.
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-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 Themenbereich, schriftliche und mündliche Präsentation
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung: schriftliche und mündliche Präsentation des Projektes (50%) und 90-minütige schriftliche Prüfung (50%)
Literaturangaben	🕮 Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011 🕮 Geschonneck, A.: Computer Forensik. dpunkt Verlag, 6. Aufl., 2014 🕮 Leitfaden IT-Forensik, Version 1.0.1, März 2011, Bundesamt für Sicherheit in der Informationstechnik, Bonn 🕮 Kuhlee, L., Völzow, V.: Computer-Forensik Hacks. O'Reilly Verlag GmbH & CO. KG, Köln, 2012 🕮 Dewald A., Freiling, F. C.: Forensische Informatik, Books on demand, Norderstedt, 1. Aufl., August 2011 🕮 Ballmann, B.: Network Hacks, Springer Vieweg, 2012 🕮 Androulidakis: Mobile Phone Security and Forensics – A practiacal Approach, Springer Science and Business Media, New York, 2012 🕮 Hayes, D.R.: A Practical Guide to Computer Forensics Investigations, Pearson Education, Inc. Indianapolis, 2015 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 9: Compliance Manager Datenschutz

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Compliance Manager Datenschutz
Kürzel	CMD
Dauer des Moduls	1 Semester
Angebotsturnus	2. Semester
Modulverantwortliche(r)	Karsten Neumann, LfDI M-V a.D.
Dozent(in)	Karsten Neumann, LfDI M-V a.D.
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Fernstudiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	keine
Qualifikationsziele des Moduls	Wissen und Verstehen Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls Kenntnisse über datenschutzrechtlicher 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. Einsatz, Anwendung und Erzeugung weiterführenden Wissens 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. Kooperation und Kommunikation 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.
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
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 Simitis, Siros: Bundesdatenschutzgesetz (Kommentar), 8. Aufl., Nomos, Baden-Baden 2014 🕮 Gohla, Peter/Schomerus, Rudolf (Hsrg.), BDSG: Bundesdatenschutzgesetz (Kommentar), 11. Aufl. Beck, München 2012 🕮 Bergmann, Möhrle, Herb, Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und Kirchen sowie zum Bereichsspezifischen Datenschutz, Loseblattwerk, ISBN 978-3-415-00616-4 🕮 Prof. Peter Gola; Dr. Georg Wronka, Handbuch Arbeitnehmerdatenschutz, Rechtsfragen und Handlungshilfen, 6. überarbeitete und erweiterte Auflage 2013, ISBN 978-3-89577-666-3 🕮 Prof. Peter Gola; RAin Yvette Reif, Praxisfälle Datenschutzrecht: Juristische Sachverhalte Schritt für Schritt prüfen, bewerten und lösen, 2. Auflage 2016, ISBN 978-3-89577-767-7 🕮 Tim Wybitul Jyn Schultze-Melling, Datenschutz im Unternehmen, 2. Auflage 2014, ISBN 9783800515721 🕮 Wilhelm Caster, Datenschutzaudit nach BSI Grundschutz, Das Praktiker-Tool für ein transparentes Datenschutzniveau in der neuen Version 2.1, 2015, ISBN 978-3-89577-765-3, 🕮 Martin Zilkens, Datenschutz in der Kommunalverwaltung, Recht - Technik – Organisation, 4., neubearb. Aufl. 2014, ISBN-13: 9783503156641, ISBN-10: 350315664X 🕮 Alexander Christl, Datenschutz im Internet: Cookies, Web-Logs, Location Based Services, eMail, Webbugs, Spyware, 2014, ISBN-13: 9783954256464, ISBN-10: 3954256460 🕮 Constanze Kurz, Frank Rieger, Die Datenfresser - Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen, Frankfurt am Main 2011, ISBN 9783100485182 🕮 Viktor Mayer-Schönberger, Delete - Die Tugend des Vergessens in digitalen Zeiten, Berlin 2010, ISBN 9783940432902

Modul 10: Industrial Security

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Industrial Security
Kürzel	IS
Dauer des Moduls	1 Semester
Angebotsturnus	3. Semester
Modulverantwortliche(r)	Prof. Dr. Nils Gruschka (FH Kiel)
Dozent(in)	Prof. Dr. Nils Gruschka (FH Kiel)
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Lehr- und Lernform	Selbststudium anhand von Lehrbriefen und *wissenschaftlicher* Literatur; Präsenzveranstaltung und 90-minütiges Webinar zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Grundkenntnisse in Mathematik, Informatik
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. Wissenschaftliches Selbstverständnis/ Professionalität 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.
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
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung: Präsentation und schriftliche Ausarbeitung
Literaturangaben	🕮 B. Vogel-Heuser, T. Bauernhansl, und M. ten Hompel, Handbuch Indust-rie 4.0 Bd.4: Allgemeine Grundlagen, 2. Aufl. Berlin: Springer Vieweg, 2016 🕮 E. D. Knapp und J. T. Langill, Industrial Network Security: Securing Criti-cal Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2 Rev ed. Waltham, MA: Syngress, 2014

Modul 11: Systemanalyse und Systemhärtung

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Systemanalyse und Systemhärtung
Kürzel	SAH
Dauer des Moduls	1 Semester
Angebotsturnus	3. Semester
Modulverantwortliche(r)	Prof. Dr.-Ing. E. Jonas
Dozent(in)	Prof. Dr.-Ing. E. Jonas
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Lehr- und Lernform	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
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Grundkenntnisse in Informatik, Mathematik, Betriebssysteme, Netzwerk- und Sicherheitsmanagement, IT-Forensik
Qualifikationsziele des Moduls	Wissen und Verstehen 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. Einsatz, Anwendung und Erzeugung von Wissen 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. Kommunikation und Kooperation Die Studierenden gewährleisten durch konstruktives, konzeptionelles Handeln die Durchführung von situationsadäquaten Lösungsprozessen. Wissenschaftliches Selbstverständnis/ Professionalität Die Studierenden entwickeln wissenschaftliche Professionalität, die sie in die Lage versetzt, ihre im Modul

	erworbenen Kenntnisse über das Thema Systemhärtung kontinuierlich zu aktualisieren.
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
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 Claudia Eckert: IT-Sicherheit, 5. Auflage, Oldenbourg-Verlag, 2007 🕮 Alexander Geschonneck: Computer-Forensic: Computerstraftaten erkennen, ermitteln, aufklären; dpunkt.verlag GmbH, 2014 🕮 Lorenz Kuhlee, Victor Völzow: Computer Forensic Hacks; O'Reilly Verlag GmbH & Co. KG, 2012 🕮 Dr. Peter Kraft: Network Hacking; Franzis Verlag GmbH, 2014 🕮 Thomas Stein: Intrusion Detection System Evasion durch Angriffsverschleierung in Exploiting Frameworks, Diplomica Verlag 2010 🕮 Jon Ericson: Hacking: Die Kunst des Exploits; dpunkt.verlag, 2008 🕮 Jochen Dinger, Hannes Hartenstein: Netzwerk- und IT-Sicherheitsmanagement: eine Einführung Taschenbuch, Universitätsverlag Karlsruhe, 2008 🕮 BSI: Leitfaden der Informationssicherheit, IT-Grundschutz kompakt 🕮 Martin Kappes: Netzwerk- und Datensicherheit, Eine praktische Einführung, Springer Vieweg, 2013 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 12: Analysemethoden für forensische Daten

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Analysemethoden für forensische Daten
Kürzel	VA
Dauer des Moduls	1 Semester
Angebotsturnus	3. Semester
Modulverantwortliche(r)	Dipl.-Ing. H.-P. Merkel
Dozent(in)	Dipl.-Ing. H.-P. Merkel
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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
Arbeitsaufwand	125 h davon 8 h Präsenzstudium
Leistungspunkte	5 CR
Voraussetzungen für die Teilnahme	Grundkenntnisse in Mathematik, Informatik, Betriebssysteme, Netzwerke, IT-Forensik
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 und auch juristische Aspekte einzubringen. <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 sowohl die technischen und juristischen Rahmenbedingungen eines IT-Forensischen Berichtes und können diese anwenden. Wissenschaftliches Selbstverständnis/ Professionalität 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.
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 praktischem, komplexen Beispiel
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung: IT-Forensischer Bericht bzgl. der Auswertung eines Beispielszenarios
Literaturangaben	🕮 Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011 🕮 Geschonneck, A.: Computer Forensik. dpunkt Verlag, 6. Aufl., 2014 🕮 Leitfaden IT-Forensik, Version 1.0.1, März 2011, Bundesamt für Sicherheit in der Informationstechnik, Bonn 🕮 Kuhlee, L., Völzow, V.: Computer-Forensik Hacks. O'Reilly Verlag GmbH & CO. KG, Köln, 2012 🕮 Dewald A., Freiling, F. C.: Forensische Informatik, Books on demand, Norderstedt, 1. Aufl., August 2011 🕮 Ballmann, B.: Network Hacks, Springer Vieweg, 2012 🕮 Androulidakis: Mobile Phone Security and Forensics – A practiacal Approach, Springer Science and Business Media, New York, 2012 🕮 Hayes, D.R.: A Practical Guide to Computer Forensics Investigations, Pearson Education, Inc. Indianapolis, 2015 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 13: Kriminalpsychologie

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Kriminalpsychologie
Kürzel	KP
Dauer des Moduls	1 Semester
Angebotsturnus	3. Semester
Modulverantwortliche(r)	Dr. S. Neick
Dozent(in)	Dr. S. Neick/FHöVPR Güstrow
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; 90-minütiges Webinar und Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand	100 h davon 8 h Präsenzstudium
Leistungspunkte	4 CR
Voraussetzungen für die Teilnahme	keine
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 und das dazugehörige Fachvokabular. Des Weiteren haben sie Kenntnisse zu Wahrnehmungs- und Gedächtnisprozessen, Emotionen und Motivationen und deren mögliche Auswirkungen auf Verhalten, ebenso wie Kenntnisse zu entwicklungspsychologischen Theorien und Modellen. Die Studierenden sind für ausgewählte Delikte insbesondere auf dem Gebiet des Cybercrimes sensibilisiert. Sie haben Wissen zu kriminalpsychologischen Aspekten, Täter und Tätertypen und ein Verständnis für normales, abweichendes und pathologisches Verhalten. <u>Einsatz, Anwendung und Erzeugung weiterführenden Wissens</u> Die Studierenden sind in der Lage, schuldmindernde und schuldausschließende Gründe bei Straftaten insbesondere auf dem Gebiet des Cybercrimes zu verstehen. 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 kriminalpsychologische Handeln in Bezug auf

	gesellschaftliche Erwartungen und Folgen zu reflektieren und entwickeln ihr berufliches Handeln entsprechend weiter.
Inhalte:	• Psychologische Grundlagen für die Erklärung menschlichen Verhaltens • Rolle von Wahrnehmungs- und Gedächtnisprozessen sowie Emotionen und Motivationen für Verhalten • Motivationen von Straftaten ausgewählter Delikte • Rolle von Entwicklungstheorien für Verhalten • Einführung in die Kriminalpsychologie • Möglichkeiten der Unterscheidung von normalem, abweichendem und pathologischem Verhalten • Überblick über Kategorisierung psychischer Störungen • Erklärungsansätze und Ursachen für die Entstehung psychischer Störungen • Zusammenhang zwischen psychischen Störungen und kriminellem Verhalten (z. B. Cybercrime) • Rechtliche Konsequenzen einer Straftat sowie schuldmindernde und schuldausschließende Gründe
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	🕮 Bondue, R.: Die Klassifikation von Brandstraftätern: eine Typologisierung anhand des Tatmotivs und anderer Variablen, Verlag für Polizeiwissenschaft Frankfurt, 2006 🕮 Dilling, H.: Mombour, W.; Schmidt, M. H.: Internationale Klassifikation psychischer Störungen. 8. Aufl., Huber Verlag, Bern 2011 🕮 Gerrig, R.: Zimbardo, P. G.: Psychologie. 20. Aufl., Pearson, Hallbergmoos, 2015 🕮 Geschonneck, A.: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 6. erw. Aufl., dpunkt.verlag, Heidelberg, 2014 🕮 Hinrichs, G.: Wer wird eigentlich delinquent? (S. 417 - 426). In Häßler, F., Kinze, W. & Nedopil, N. (Hrsg.): Praxishandbuch Forensische Psychiatrie. 2. Aufl., Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin, 2015 🕮 Kury, H. ; Obergfell-Fuchs, J.: Rechtspsychologie. Forensische Grundlagen und Begutachtung. Ein Lehrbuch für Studium und Praxis. 1. Aufl., Kohlhammer, Stuttgart, 2012 🕮 Nedopil, N.: Begutachtungen zur Frage von Schuldunfähigkeit und verminderter Schuldfähigkeit (S. 352 – 368). In Bliesener, T., Lösel, F. & Köhnken, G.: Lehrbuch Rechtspsychologie. 1. Aufl., Huber, Bern, 2014 🕮 Suhling, S. & Greve, W.: Kriminalpsychologie kompakt. Beltz, Weinheim, 2010 🕮 Sticher-Gil, B.: Polizei- und Kriminalpsychologie. 2. Aufl., Verlag für Polizeiwissenschaft, Frankfurt am Main 2007 🕮 Suhling, S. & Greve, W.: Kriminalpsychologie kompakt. Beltz, Weinheim, 2010

Modul 14: Ethische Probleme der Informationstechnologie

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Ethische Probleme der Informationstechnologie
Kürzel	EPI
Dauer des Moduls	1 Semester
Angebotsturnus	3. Semester
Modulverantwortliche(r)	Dr. phil. Roland Reiske
Dozent(in)	Dr. phil. Roland Reiske
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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
Arbeitsaufwand	100 h davon 8 h Präsenzstudium
Leistungspunkte	4 CR
Voraussetzungen für die Teilnahme	keine
Qualifikationsziele des Moduls	Wissen und Verstehen Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls Kenntnisse über ethische Grundpositionen und über 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 ethisches Handeln in Bezug auf gesellschaftliche Erwartungen und Folgen zu reflektieren und entwickeln ihr berufliches Handeln entsprechend weiter. Des Bewusstseins für die Notwendigkeit ethischer Normen und der Ausrichtung menschlicher Handlungen wurde bei den Studierenden geschärft.
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 Informationen, ihre Erhebung, Speicherung, Übermittlung, Verarbeitung und Nutzung beziehen. Das Ziel ist die Schärfung des Bewusstseins für die Notwendigkeit ethischer Normen und

	der Ausrichtung menschlicher Handlungen – und der anderer Vernunftwesen (KI, autonome Steuerungen etc.) – an ihnen.
Voraussetzungen für die Vergabe von Leistungspunkten	120-minütige schriftliche Prüfung
Literaturangaben	**Einführungen:** 📖 Frankena, William K.: Analytische Ethik: Eine Einführung, DTV, 1986 📖 Rüdiger Funiok: Medienethik: Verantwortung in der Mediengesellschaft, Kohlhammer, 2007 📖 Herlinde Pauer-Studer: Einführung in die Ethik, UTB, 2010 📖 Pieper/Turnherr: Angewandte Ethik: Eine Einführung, Beck, 1998 📖 Gunzelin Schmid Noerr: Geschichte der Ethik, Reclam, 2006 **Basistexte Ethik:** 📖 Aristoteles: Die Nikomachische Ethik, DTV, 1991 📖 David Hume: Ein Traktat über die menschliche Natur Buch II/III, Meiner, 1978 📖 Immanuel Kant: Grundlegung zur Metaphysik der Sitten, Meiner, 1999 📖 John Stuart Mill: Der Utilitarismus, (Utilitarianism) Reclam, 2006 📖 Platon: Apologie & Kriton in: Werke Bd. 1, Rowohlt, 1994 📖 Smart/Williams: Utilitarianism for and against, Cambridge, 2005 **Informatik & Ethik:** 📖 Michael Nagenborg: Das Private unter den Rahmenbedingungen der IuK-Technologie: Ein Beitrag zur Informationsethik, 2005 📖 Deborah Weber-Wulff / Christina Class u.a.: Gewissensbisse: Ethische Probleme der Informatik. Biometrie - Datenschutz - geistiges Eigentum, 2009 📖 William Brinkman / Altan F. Sanders: Ethics in a Computing Culture, 2012 📖 Joseph Migga Kizza: Ethical and Social Issues in the Information Age, 2012

Modul 15: Masterseminar

Studiengang	IT-Sicherheit und Forensik
Modulbezeichnung	Masterseminar
Kürzel	MS
Dauer des Moduls	1 Semester
Angebotsturnus	3. Semester
Modulverantwortliche(r)	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in)	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache	Deutsch
Verwendbarkeit des Moduls	Pflichtmodul im Master-Studiengang „IT-Sicherheit und Forensik“
Lehr- und Lernform	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
Arbeitsaufwand	50 h davon 8 h Präsenzstudium
Leistungspunkte	2 CR
Voraussetzungen für die Teilnahme	keine
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. Wissenschaftliches Selbstverständnis/ Professionalität Die Studierenden entwickeln ein berufliches Selbstbild weiter, das sich an Zielen und Standards professionellen Handelns sowohl in der Wissenschaft als auch den Berufsfeldern

	außerhalb der Wissenschaft orientiert. Sie können das eigene Handeln/ die eigenen Ideen mit theoretischem und methodischem Wissen begründen und reflektieren es hinsichtlich alternativer Entwürfe.
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
Voraussetzungen für die Vergabe von Leistungspunkten	Alternative Prüfungsleistung: Exposé und 15min-Vortrag zum geplanten Thema der Master Thesis
Literaturangaben	🕮 Theuerkauf, J.: Schreiben im Ingenieurstudium: Effektiv und Effizient zu Bachelor-, Master- und Doktor-Arbeit, UTB GmbH; Auflage: 1. Aufl. (18. Juli 2012) 🕮 Prevezanos, C.: Technisches Schreiben - Für Informatiker, Akademiker, Techniker und den Berufsalltag, Carl Hanser Verlag München, 2013 🕮 Fachspezifische Literatur entsprechend des gewählten Forschungsgebietes

Modul 16: Master Thesis

Studiengang:	IT-Sicherheit und Forensik
Modulbezeichnung (Deutsch):	Master Thesis
Kürzel	MT
Semester:	1 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	1. und 2. Prüfer sind Dozent im Studiengang Master „IT-Sicherheit und Forensik“ oder 1. Prüfer ist Dozent im Studiengang Master „IT-Sicherheit und Forensik“ und 2. Gutachter ist ein externer Gutachter
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Master-Studiengang IT-Sicherheit und Forensik
Lehrform:	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.
Arbeitsaufwand:	500 Stunden (499 h 15 min. Selbststudium und 45 min. Kolloquium)
Kreditpunkte:	20 CR
Voraussetzungen:	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.
Lernziele / Kompetenzen:	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.
Inhalt:	Es handelt sich um eine praxisbezogene theoretische Auseinandersetzung mit aktuellen und/oder wissenschaftlichen 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.
Studien- Prüfungsleistungen:	Wiss. Arbeit (Master-Thesis) und 45min Kolloquiums (30min Präsentation und 15min Diskussion zum Bachelor-Thema)
Literatur:	📖 wird entsprechend des Themas gewählt