Modultitel: **Modultyp:** **Englische Übersetzung:**	**Cybersecurity 1** **Wahlpflichtmodul** **Cybersecurity 1**
Qualifikationsziele Die Gliederung der Kompetenzbereiche erfolgt analog der Gliederung des Qualifikationsrahmens für deutsche Hochschulabschlüsse (**HQR**, 2017)	Gesamtqualifikationsziel: Mit Hilfe der Modulkombination Cybersecurity 1 und 2 bauen die Studierenden theoretische und praktische Kenntnisse zur Absicherung von Computersystemen gegen Angriffe auf. Diese Kenntnisse werden mit Hilfe praktischer Angriffsszenarien auf gekapselte Laborsysteme vertieft. Cybersecurity 1 fokussiert auf theoretische Grundlagen und Softwaresicherheit, Cybersecurity 2 auf vernetzte Systeme und Managementmaßnahmen zur Sicherheitserhöhung. Die alleinige Belegung von Cybersecurity 1 ist möglich. Fachkompetenz (Wissen und Verstehen) • Es wird ein Grundverständnis über theoretische Maßnahmen und Methoden zur Sicherheit digitaler Systeme aufgebaut. • Die Bedeutung unterschiedlicher kryptographischer Methoden und Elemente für Cybersecurity wird verstanden. • Nutzeridentität und Identitätsmanagement bzgl. Zugriffskontrolle werden verstanden. • Angriffsmethoden, -detektion und -abwehr werden verstanden. <u>Methodenkompetenz</u> (Einsatz, Anwendung und Erzeugung von Wissen) Ausgewählte Inhalte werden mit praktischen Methoden zu cyberphysikalischen Angriffen auf spezielle gekapselte, präparierte Systeme geübt. Dieses Wissen dient dazu, IT-Systeme sicher zu gestalten und Angreifer fernzuhalten. <u>Sozialkompetenz</u> (Kommunikation und Kooperation) Die Studierenden werden in die Lage versetzt, Probleme selbstständig und im Team zu bearbeiten <u>Selbstkompetenz</u> (Wissenschaftliches Selbstverständnis /Professionalität) Studierende werden dazu in die Lage versetzt, selbstständig Sicherheitsmaßnahmen in IT-Systemen zu evaluieren und zu optimieren. Darüber hinaus sind sie in der Lage, sich in dem dynamisch verändernden Gebiet der Sicherheitsbedrohungen selbstständig weiterzubilden.
Inhalte	1. Rechtliche und ethische Aspekte der Cybersecurity (CS) 2. Grundbegriffe und Motivation der CS 3. Einsatz kryptographischer Methoden in der CS 4. Nutzeridentifikation und Zugriffkontrolle 5. Prinzipien von Schadsoftware 6. Gängige Angriffsvektoren 7. Softwaresicherheit 8. Betriebssystemsicherheit

	9. Detektions- und Abwehrszenarien
Lehrformen	2V mit integrierten praktischen Übungseinheiten
Unterrichtssprache	Deutsch oder Englisch Die Materialien werden vornehmlich in englischer Sprache zur Verfügung gestellt
Voraussetzungen für die Teilnahme	<u>Erforderlich:</u> Notwendige fachliche Voraussetzungen sind die Kenntnisse eines Bachelorstudiums mit Ingenieurschwerpunkt mit den Fächern Mathematik 1 und 2, Programmieren, Rechnerarchitekturen. Ausreichende englische Sprachfähigkeiten, um der Vorlesung ggf. auch in englischer Sprache folgen zu können und englischsprachige Materialien verstehen zu können. <u>Empfohlen:</u> Empfohlene fachliche Voraussetzungen sind die Kenntnisse über oder das parallele Belegen von Veranstaltungen zur Sicherheit in verteilten Systemen (z.B. DLT) oder vernetzten Systemen (z.B. drahtlose Sensornetze.
Verwendbarkeit des Moduls	Wahlpflichtmodul im IT-Schwerpunkt eines Masterstudienganges
Art, Voraussetzung und Sprache der Modulprüfung	Regelhafte Prüfungsform für die Modulprüfung: PL Abschlussprüfung in Form einer Klausur von 1,5 Stunden Dauer Voraussetzung für die Teilnahme an der Prüfung: erfolgreiches Absolvieren der Praxisanteile der Vorlesung Weitere mögliche Prüfungsformen: Mündliche Prüfung, Referat, Hausarbeit Bei mehr als einer möglichen Prüfungsform im Modul wird die zu erbringende Prüfungsform von dem verantwortlichen Lehrenden zu Beginn der Lehrveranstaltung bekannt gegeben.
Gesamtarbeitsaufwand	3 Leistungspunkte (LP) 2 Semesterwochenstunden (SWS) Gesamtarbeitsaufwand 90 h, davon Präsenzstudium 36 h, 16 Stunden Laborvorbereitung im Selbststudium und 38 h Vorlesungsvor- und -nachbereitung sowie Prüfungsvorbereitung im Selbststudium
Häufigkeit des Angebots	Einmal pro Jahr
Dauer	2 SWS über ein Semester
Literatur	[1] D. Basin, P. Schaller, und M. Schläpfer, *Applied information security: a hands-on approach*. Heidelberg ; New York: Springer, 2011. [2] W. Stallings und L. Brown, *Computer security: principles and practice*, Fourth Edition, Global edition. New York, NY: Pearson, 2018. [3] R. Boyle und R. R. Panko, *Corporate computer security.* 2015.

	[4] P. Engebretson, *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*, Second Edition. Amsterdam ; Boston: Syngress, an imprint of Elsevier, 2013.