

<b>Modultitel:</b> <b>Modultyp:</b> <b>Englische Übersetzung:</b>	<b>Cybersecurity 2</b> <b>Wahlpflichtmodul</b> <b>Cybersecurity 2</b>
<p>Qualifikationsziele</p> <p>Die Gliederung der Kompetenzbereiche erfolgt analog der Gliederung des Qualifikationsrahmens für deutsche Hochschulabschlüsse (HQR, 2017)</p>	<p>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.</p> <p><u>Fachkompetenz</u> (Wissen und Verstehen)          Aufbauend auf dem Kurs Cybersecurity1 werden ergänzend folgende Fachkompetenzen:</p> <ul style="list-style-type: none"> <li>• Wissen über gängige Netzwerkprotokolle und -anwendungen.</li> <li>• Verständnis über Besonderheiten in der Sicherheit drahtloser Netzwerke.</li> <li>• Wissen über organisatorische Maßnahmen, um die IT-Sicherheit zu erhöhen.</li> <li>• Kenntnis von Verfahren zu Überprüfung, Abnahme und Zertifizierung von IT-Sicherheit.</li> </ul> <p><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.</p> <p><u>Sozialkompetenz</u> (Kommunikation und Kooperation)          Die Studierenden werden in die Lage versetzt, Probleme selbstständig und im Team zu bearbeiten</p> <p><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 die Sicherheitsbedrohungen selbstständig weiterzubilden.</p>
<p>Inhalte</p>	<ol style="list-style-type: none"> <li>1. Internetanwendungen, -protokolle und Standards</li> <li>2. Maßnahmen und Anwendungen zur Sicherheitserhöhung in Internet</li> <li>3. Besonderheiten drahtloser Netzwerke</li> <li>4. Sicherheitsmanagement und Bewertung in Unternehmen</li> <li>5. Sicherheitsmaßnahmen und -pläne</li> <li>6. Absicherung der physischen Infrastruktur</li> <li>7. Absicherung des Personals</li> <li>8. Sicherheitsaudits</li> </ol>

Modulhandbuch des M.Sc. Wirtschaftsingenieurwesen

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

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