

Ruhr-Universität Bochum (RUB)

Mikromodulnummer	3007																					
Studienprogramm	Zertifikatsprogramm																					
Mikromodulbezeichnung:	WWW-Sicherheit mit SSL (Thema: Netzsicherheit 2)																					
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk																					
Dozent(in):	Prof. Dr. Jörg Schwenk, Christopher Späth, Sebastian Lauer																					
Sprache:	Deutsch																					
Zeitaufwand:	<p>Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: right;">Präsenzstudium:</td> <td style="width: 10%;"></td> <td style="text-align: right;">Zeitstunden</td> </tr> <tr> <td style="text-align: right;"> davon Prüfung und Prüfungsvorbereitung:</td> <td style="text-align: center;">0</td> <td style="text-align: right;">Zeitstunden</td> </tr> <tr> <td style="text-align: right;">Fernstudienanteil:</td> <td style="text-align: center;">51</td> <td style="text-align: right;">Zeitstunden</td> </tr> <tr> <td style="text-align: right;"> davon Selbststudium:</td> <td style="text-align: center;">40</td> <td style="text-align: right;">Zeitstunden</td> </tr> <tr> <td style="text-align: right;"> davon Aufgaben:</td> <td style="text-align: center;">9</td> <td style="text-align: right;">Zeitstunden</td> </tr> <tr> <td style="text-align: right;"> davon Online-Betreuung:</td> <td style="text-align: center;">2</td> <td style="text-align: right;">Zeitstunden</td> </tr> <tr> <td style="text-align: right;">Summe:</td> <td style="text-align: center;">51</td> <td style="text-align: right;">Zeitstunden</td> </tr> </table>	Präsenzstudium:		Zeitstunden	davon Prüfung und Prüfungsvorbereitung:	0	Zeitstunden	Fernstudienanteil:	51	Zeitstunden	davon Selbststudium:	40	Zeitstunden	davon Aufgaben:	9	Zeitstunden	davon Online-Betreuung:	2	Zeitstunden	Summe:	51	Zeitstunden
Präsenzstudium:		Zeitstunden																				
davon Prüfung und Prüfungsvorbereitung:	0	Zeitstunden																				
Fernstudienanteil:	51	Zeitstunden																				
davon Selbststudium:	40	Zeitstunden																				
davon Aufgaben:	9	Zeitstunden																				
davon Online-Betreuung:	2	Zeitstunden																				
Summe:	51	Zeitstunden																				
Leistungspunkte	keine																					
Voraussetzungen:	Mikromodul "Kryptographie und Internet"																					
Lernziele/Kompetenzen	<p>Fachkompetenz: Die Studierenden verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln. Die Studenten können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern.</p> <p>Methodenkompetenz: Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können.</p> <p>Sozialkompetenz: Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.</p> <p>Selbstkompetenz: Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Die Studenten entwickeln ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten.</p>																					
Lehrinhalt	<p>Das Hypertext Transfer Protocol (HTTP) HTTP-Sicherheitsmechanismen Secure HTTP Erste Versuche: SSL 2.0 und PCT SSL 3.0: Sicherheitsschicht über TCP SSL Record Layer SSL Handshake SSL Alert Protocol TLS: Der Internet-Sicherheitsstandard Angriffe auf SSL Formale Analysen von TLS Praktische Aspekte</p>																					
Studien- und Prüfungsleistungen:	keine																					
Medienformen:	Onlineveranstaltung: flexible Vertiefung wichtiger Themen, Lernen im Dialog, elektronischer Studienbrief																					
Literatur:	Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.																					