

## Kostenfreie Pilotierung der Mikromodule des Zertifikatsprogramms Open C<sup>3</sup>S

### Mikromodul MM-3007 „WWW-Sicherheit mit SSL“ aus Netzsicherheit 2

Kryptographie und das Internet    Ruhr-Universität Bochum

<b>Abschluss</b>	Teilnahmebescheinigung / keine ECTS-Punkte
<b>Studienort</b>	online-basiert (ohne Präsenzveranstaltung)
<b>Zulassung</b>	ohne Zulassungsvoraussetzungen
<b>Bewerbungsfrist</b>	<b>04.04.2017</b>
<b>Selbststudium</b>	Erarbeiten der Lehrinhalte im Selbststudium
<b>Gesamtworkload</b>	51 h
<b>Online-Veranstaltungen</b>	<b>1. Termin am 12.04.2017</b> <b>2. Termin am 24.04.2017</b>
<b>Gebühren</b>	Die Teilnahme am Mikromodul ist in der Pilotphase <b>gebührenfrei</b>
<b>Verpflichtung</b>	Verpflichtung zur Teilnahme an der <b>Evaluation</b> des Mikromoduls anhand eines Fragebogens
<b>Besonderheiten</b>	Online basiertes Mikromodul, Betreuung über Tutoren, Fragen zu den Inhalten über den Chat
<b>An wen wendet sich das Modul</b>	Berufstätige, die ihr Fachwissen erweitern wollen
<b>Empfohlene Voraussetzungen</b>	Mikromodul „Kryptographie und Internet“
<b>Lerninhalt und angestrebte Lernergebnisse</b>	<p><b>Fachkompetenz:</b> Die Studierenden verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln.</p> <p>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><b>Methodenkompetenz:</b> Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können.</p> <p><b>Sozialkompetenz:</b> Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.</p> <p><b>Selbstkompetenz:</b> 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>
<b>Lehrinhalt</b>	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
<b>Anmeldung bis 04.04.2017 bei</b>	Frau Sabine Merz über <a href="mailto:merzs@hs-albsig.de">merzs@hs-albsig.de</a> (Bitte Anmeldeformular anfordern)