

**Kostenfreie Pilotierung des Zertifikatsprogramms Open C³S in der 2. Förderphase
 MODUL Z-801 “Cloud-Sicherheit und Cloud-Forensik mit
 Schwerpunkt Angriffsanalyse“ bestehend aus 5 Mikromodulen**

Modul Z-801	Universität Passau
Abschluss Z-801	Bei Teilnahme am kompletten Modul Z-801 (inkl. aller nachstehend genannten Mikromodule) mit erfolgreicher Abschlussprüfung erhalten Sie ein Hochschulzertifikat und 5 ECTS-Punkte
Studienort	Online-basiert, Präsenzveranstaltung am 20. Und 21. Mai 2017 an der Universität Passau
Prüfung	Für das Modul Z-801 findet am 22. Juli 2017 eine Prüfung in Präsenz statt. Standorte werden Passau, Bochum und Albstadt sein
Zulassung	Ohne Zulassungsvoraussetzungen
Bewerbungsfrist	24. April 2017
Selbststudium	Erarbeiten der Lehrinhalte im Selbststudium
Gesamtworkload	150 h (jeweils 30 h pro Mikromodul)
Gebühren	Die Teilnahme am Modul ist in der Pilotphase gebührenfrei
Verpflichtung	Verpflichtung zur Teilnahme an der Evaluation der Mikromodule anhand eines Online-Fragebogens
Besonderheiten	Online-basiertes Modul, Betreuung über Tutoren, Fragen zu den Inhalten über das Betreuerforum
Anmeldung bis 24. April 2017 bei	Frau Sabine Merz über merz@hs-albsig.de Bitte Anmeldeformular anfordern

Mikromodul MM-8001

„Grundlagen von Virtualisierungstechnik und Cloud-Computing“

Online-Veranstaltung	8. Mai 2017, 17: 00 Uhr
Gesamtworkload	30 h
Prüfung	Für das Modul Z-801 (inkl. aller Mikromodule) findet am 22. Juli 2017 eine Prüfung in Präsenz statt. Standorte werden Passau, Bochum und Albstadt sein
Lernziele/Kompetenzen	Nach Abschluss dieses Mikromoduls können Sie unterschiedliche Konzepte von Virtualisierung unterscheiden und sind mit den Konzepten und Architekturen von Rechnervirtualisierung vertraut. Ihnen sind die verschiedenen Definitionen des Begriffs „Cloud Computing“ vertraut und Sie verfügen über ein vertieftes Verständnis über die wesentlichen Service- und Verarbeitungsmodelle. Sie können die Unterschiede zwischen diesen Modellen, insbesondere hinsichtlich von Sicherheitsfragen, beurteilen.
Lehrinhalt	Geschichtliche Hintergründe von Virtualisierungstechnik Virtualisierungsarten (Rechner-, Betriebssystem-, Netz-, und Anwendungsvirtualisierung); Details von Rechnervirtualisierung mit Intel- und ARM-Hardware; Service-Modelle und Verarbeitungsmodelle von Cloud Computing nach NIST

Mikromodul MM-8002

„Cloud-Sicherheit und Bedrohungsmodelle“

Online-Veranstaltung	Termin wird nachgereicht
Gesamtworkload	30 h
Prüfung	Für das Modul Z-801 (inkl. aller Mikromodule) findet am 22. Juli 2017 eine Prüfung in Präsenz statt. Standorte werden Passau, Bochum und Albstadt sein
Lernziele/Kompetenzen	Nach Abschluss dieses Mikromoduls sind sie mit den Grundlagen von Bedrohungsmodellierung und Risikomanagement in IT-Systemen vertraut. Auf dieser Grundlage können Sie Sicherheitsherausforderungen in Cloud-Infrastrukturen beurteilen. Sie sind vertraut mit technischen Ansätzen zur sicheren Speicherung und Verarbeitung von Daten in der Cloud. Sie haben ein grundlegendes Verständnis für die Gefahr durch Seitenkanalangriffe in der Cloud.
Lehrinhalt	Bedrohungsmodellierung und Risikomanagement, Sicherheitsherausforderungen in der Cloud, Sichere Datenspeicherung in der Cloud, Sichere Datenverarbeitung in der Cloud, Koresidenz und Seitenkanalangriffe in virtualisierungsbasierten Infrastrukturen

Mikromodul MM-8003

„Grundlagen von Cloud-Forensik“

Online-Veranstaltung	15. Mai 2017, 17: 00 Uhr
Gesamtworkload	30 h
Prüfung	Für das Modul Z-801 (inkl. aller Mikromodule) findet am 22. Juli 2017 eine Prüfung in Präsenz statt. Standorte werden Passau, Bochum und Albstadt sein
Lernziele/Kompetenzen	Nach Abschluss dieses Mikromoduls kennen Sie die Grundlagen von Techniken der IT-Forensik sowie die dazugehörigen Vorgehensmodelle. Sie überblicken die Herausforderungen und Möglichkeiten der forensischen Untersuchung bei cloudbasierter Datenspeicherung sowie bei virtuellen Maschinen. Darüber hinaus verfügen Sie über Kenntnisse zum aktuellen Stand der Forschung zu Forensik unterstützenden Cloud-Diensten und sind mit der „Forensic Readiness“ vertraut.
Lehrinhalt	Historische Entwicklung von IT-Forensik Aktuelle Modelle der IT-Forensik Datenträger-Forensik in der Cloud Live-Forensik in der Cloud Forensik-Dienste und Forensik-Readiness-Modelle in der Cloud

Mikromodul MM-8004

„Virtual Machine Introspection“

Online-Veranstaltung	29. Mai 2017, 17: 00 Uhr
Gesamtworkload	30 h
Prüfung	Für das Modul Z-802 (inkl. aller Mikromodule) findet am 22. Juli 2017 eine Prüfung in Präsenz statt. Standorte werden Passau, Bochum und Albstadt sein
Lernziele/Kompetenzen	Nach Bearbeitung dieses Mikromoduls sind Sie mit Theorie und Praxis von Virtual Maschine Introspection (VMI) vertraut. Sie kennen die grundlegende Funktionsweise und Anwendungsmöglichkeiten von VMI. Sie haben ein vertieftes Verständnis für das Problem der semantischen Lücke (semantic gap) erlangt und können auf dieser Grundlage die Grenzen und Risiken einer Fehlinterpretation bei VMI einschätzen. Sie sind mit dem Werkzeug Volatility vertraut, um laufende virtuelle Maschinen mit existierenden Plug-Ins zu untersuchen und einfache Plug-Ins selbst zu entwickeln bzw. zu erweitern.
Lehrinhalt	Grundlagen, Herausforderungen und Anwendungsmöglichkeiten von VMI, Funktionsweise von LibVMI, Untersuchung von Linux-Kernel-Datenstrukturen mit Volatility, Untersuchung laufender virtueller Maschinen mit Volatility und LibVMI

Mikromodul MM-8005

„Einbruchserkennung und Honeypots in der Cloud“

Online-Veranstaltung	26. Juni 2017, 17: 00 Uhr
Gesamtworkload	30 h
Prüfung	Für das Modul Z-801 (inkl. aller Mikromodule) findet am 22. Juli 2017 eine Prüfung in Präsenz statt. Standorte werden Passau, Bochum und Albstadt sein
Lernziele/Kompetenzen	Nach Bearbeitung dieses Mikromoduls kennen Sie die Grundbegriffe und Funktionsweisen von Einbrucherkennungs-systemen (Intrusion Detection System – IDS) und von Honeypots. Sie sind vertraut mit den Möglichkeiten, wie sich IDS in Cloud-Umgebungen verwenden lassen. Zudem sind Sie in der Lage, Honeypot-Systeme in der Cloud zu betreiben und deren Vor- und Nachteile zu beurteilen.
Lehrinhalt	Grundlagen von IDS-Systemen Grundlagen von Honeypots IDS in der Cloud Honeypots in der Cloud