18 Sicherheitsmanagement

Security Gorvernance

Semester	3
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Ivo Keller
Teilnahmevoraussetzungen	Grundlagen der IT-Sicherheit
Lernergebnisse	Die Studierenden haben nach Abschluss des Moduls verstanden, dass Sicherheitsanforderungen eine ganzheitliche Sichtweise bedingen und nach Effektivitäts- und Effizienzkriterien umgesetzt werden. Die Studierenden sind final in der Lage, • die tragenden Geschäftsprozesse zu analysieren und daraus die Unternehmenswerte abzuleiten, • eine IT-Infrastruktur und den Netzwerkverkehr zu analysieren, • eine Angreifer-, bzw. Bedrohungsmodellierung durchzuführen, • das Risiko für Unternehmens-, Software-Entwicklungs- und ggf. auch für Software-Prozesse einzuschätzen, zu priorisieren und effektive und effiziente Maßnahmen vorzuschlagen, • die Verhältnismäßigkeit der Gegenmaßnahmen zu erklären. Sie kennen und können anwenden: • organisatorische Sicherheits-Maßnahmen, • BSI-Standards und ISO-Normen, wie die 27000er Familie, • kryptographische Verfahren, das Identitäts- und Zugriffsmanagement (IAM) sowie die Public Key Infrastruktur (PKI).
Prüfungsvorleistung	wird zu Beginn des Sem. bekannt gegeben
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Web-Konferenz, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 120 h Webkonferenzteilnahme: ca. 26 h

	Präsenzteilnahme: ca. 4 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	inhaltliche Klärung, Vorstellung des Lösungskonzepts des Projekts
Prüfungsform	
Literatur	Sachar Paulus: „Basiswissen Sichere Software“, dpunkt.verlag, 2011 Heinrich Kersten: „IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls“, 2016 (978-3658146931) Müller, Klaus-Rainer: „IT-Sicherheit mit System“, 5. Aufl., Springer Vieweg, 2014 Adam Shostack: „Threat Modeling: Designing for security“, Wiley, 2014 Michael Howard: „Sichere Software programmieren“, Microsoft Press, 2002 Microsoft Security Development Lifecycle (SDL), 2012, https://msdn.microsoft.com/en-us/library/windows/desktop/cc307748.aspx Microsoft: „The STRIDE Threat Model“, 2005 http://msdn.microsoft.com/library/ms954176.aspx Claudia Eckert: „IT-Sicherheit. Konzepte - Verfahren – Protokolle“, Oldenbourg, 2009, http://www.worldcat.org/oclc/463676855
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Sicherheitsmanagement betrachtet die Sicherheits-Effizienz und Effektivität ganzheitlich: In der Hierarchie Unternehmen, Software-Lebenszyklus, Code werden jeweils zunächst der Schutzbedarf analysiert, bevor sinnvolle Maßnahmen geplant werden. Software-Sicherheit gewinnt als Qualitätsziel ständig an Bedeutung. **Kapitel** • Ganzheitliches Sicherheitsmanagement • Software-Qualität und Sicherheits-Anforderungen • Compliance und Normen • Bedrohungsmodellierung im Unternehmen, Software Development Lifecycle und Code • Risikomanagement • Sichere agile Organisation und DevOps • Security Frameworks • Auslieferung und Wartung