Modulübersicht

ZERTIFIKATSLEHRGANG **IT-SECURITY ENGINEERING**

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber

TECHNISCHE HOCHSCHULE NÜRNBERG
OHM PROFESSIONAL SCHOOL

Studieninhalte

Zertifikat IT-Security Engineering

Risk Assessment und Security Requirements	
Vertiefung	SEC
Nummer	SEC-V1
Lehrveranstaltung	3 SU, 1 Ü
Modulverantwortlicher	Patrick Seubelt, M.Eng.
Arbeitsbelastung	Es wird angenommen, dass durchschnittliche Studierende 75 Stunden Arbeitsaufwand benötigen, um sich die genannten Kenntnisse und Fähigkeiten anzueignen. Diese verteilen sich wie folgt: ▪ 45 Std. Präsenz in Lehrveranstaltungen und Übungen ▪ 15 Std. regelmäßige Nachbereitung des Lehrstoffes ▪ 45 Std. Erstellung von Übungsprogrammen und Programmlösungen ▪ 25 Std. Literaturstudium und freies Arbeiten ▪ 20 Std. Prüfungsvorbereitung Daraus ergeben sich 5 Leistungspunkte.
SWS / Leistungspunkte	4 SWS / 5 ECTS
Leistungsnachweise	Klausur 120 min
Voraussetzungen	▪ Kenntnisse und Fähigkeiten auf Bachelorniveau im IT-Bereich ▪ Berufliche Tätigkeit in der SW-Entwicklung ▪ Kenntnis und Erfahrung mit den gängigsten Entwicklungswerkzeugen und Sprachen (C++, C#, Java, Javascript, Visual Studio, RAD)

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber

Studieninhalte

Zertifikat IT-Security Engineering

Risk Assessment und Security Requirements

Lernziele	▪ Die Studierenden lernen typische Schwachstellen in IT Systemen und Anwendungen kennen. Sie erlernen, wie die entsprechenden Schwachstellen ermittelt und wie sie ausgenutzt werden können ▪ Die Studierenden sollen verstehen, wie IT Sicherheitsanalysten innerhalb des IT Security Managements eines Unternehmens Schwachstellen melden, Risiken klassifizieren, bewerten und beschreiben ▪ Die Studierenden sollen lernen, Risikofaktoren und Schadenspotentiale in der Entwicklung und dem Betrieb von Softwaresystem zu erkennen und zu bewerten ▪ Die Studierenden sollen lernen, aus ermittelten Angriffsmöglichkeiten und Schwach-stellen gezielt Requirements für die Softwareentwicklung und Wartung zu eruieren und diese für die Entwicklungsphasen Design und Development zu dokumentieren

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber

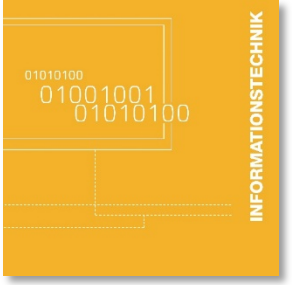
Studieninhalte

Zertifikat IT-Security Engineering

Risk Assessment und Security Requirements

Inhalt	▪ Es wird aufgezeigt, welche Auswirkungen Sicherheitsprobleme in der Unternehmens-IT haben können: was die schützenwerten Güter sind und warum sie geschützt werden sollen ▪ Welche Motivation führt zum Angriff auf schützenswerte Güter, wie laufen professionelle Angriffe auf die IT eines Unternehmens ab und welche Zielsetzungen verfolgen Angreifer dabei: wie denkt ein Angreifer und wie geht er vor ▪ Welche Anforderungen ergeben sich für die Softwareentwicklung aus den Angriffs-möglichkeiten und typischen Angriffspunkten und wie sind diese zu dokumentieren ▪ Quellen für Security Requirements erschließen ▪ Welche Ergebnisse der Bedrohungs- und Risikoanalyse sind zum Aufstellen von Security Requirements zu benutzen ▪ Schutzprofile und Sicherheitsvorgaben analysieren ▪ Wie Sicherheitsanforderungen von Stakeholdern (Nutzer, Sicherheitsverantwortliche, Sicherheitsberater, ...) analysiert werden

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber



Studieninhalte

Zertifikat IT-Security Engineering

Governance Frameworks & Standards	
Vertiefung	SEC
Nummer	SEC-V2
Lehrveranstaltung	3 SU, 1 Ü
Modulverantwortlicher	Christian S. Fötinger, M.Sc.
Arbeitsbelastung	Es wird angenommen, dass durchschnittliche Studierende 75 Stunden Arbeitsaufwand benötigen, um sich die genannten Kenntnisse und Fähigkeiten anzueignen. Diese verteilen sich wie folgt: ▪ 45 Std. Präsenz in Lehrveranstaltungen und Übungen ▪ 15 Std. regelmäßige Nachbereitung des Lehrstoffes ▪ 45 Std. Erstellung von Übungsprogrammen und Programmlösungen ▪ 25 Std. Literaturstudium und freies Arbeiten ▪ 20 Std. Prüfungsvorbereitung Daraus ergeben sich 5 Leistungspunkte.
SWS / Leistungspunkte	4 SWS / 5 ECTS
Leistungsnachweise	Klausur 120 min
Voraussetzungen	Kenntnisse und Fähigkeiten aus dem Modul Risk Assessment (SEC-V1)

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber

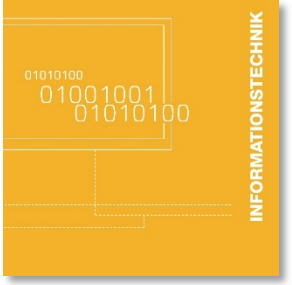
Studieninhalte

Zertifikat IT-Security Engineering

Governance Frameworks & Standards

Lernziele	▪ Die Studierenden erlernen, welche rechtlichen Grundlagen, Industriestandards und Best Practices bei der Verarbeitung von Daten und dem Umgang mit Informationen relevant sind und wie IT-Systeme und Anwendungen vor diesem Hintergrund betrieben werden ▪ Die Studierenden erlernen, welche Standards welche Sicherheitsanforderungen abdecken und wo in aktuellen Standardverfahren diese Anforderungen noch nicht ausreichend behandelt sind ▪ Die Studierenden lernen Methoden und Werkzeuge kennen, um diese Anforderungen in die Praxis umzusetzen
Inhalt	▪ Grundlagen der Informationssicherheit und des Datenschutzes ▪ Prüf- und Melde- und Dokumentationspflichten aus regulatorischer Perspektive ▪ Die Bewertung von Reifegraden gegenüber Standards ▪ Welche Überwachungsprozeduren und Maßnahmen finden zur Einhaltung von Vor- gaben Anwendung und werden gegenüber internen und externen Stakeholdern dokumentiert und berichtet ▪ Es wird aufgezeigt, in welchen Bereichen die Einhaltung von Standards und Best Practices bereits aktuelle Sicherheitsanforderungen behandelt ▪ Wo sind ggf. Sonderverfahren oder spezifische Einzelmaßnahmen notwendig

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber



Studieninhalte

Zertifikat IT-Security Engineering

Security Design	
Vertiefung	SEC
Nummer	SEC-V3
Lehrveranstaltung	3 SU, 1 Ü
Modulverantwortlicher	Christian S. Fötinger, M.Sc.
Arbeitsbelastung	Es wird angenommen, dass durchschnittliche Studierende 75 Stunden Arbeitsaufwand benötigen, um sich die genannten Kenntnisse und Fähigkeiten anzueignen. Diese verteilen sich wie folgt: ▪ 45 Std. Präsenz in Lehrveranstaltungen und Übungen ▪ 15 Std. regelmäßige Nachbereitung des Lehrstoffes ▪ 45 Std. Erstellung von Übungsprogrammen und Programmlösungen ▪ 25 Std. Literaturstudium und freies Arbeiten ▪ 20 Std. Prüfungsvorbereitung Daraus ergeben sich 5 Leistungspunkte.
SWS / Leistungspunkte	4 SWS / 5 ECTS
Leistungsnachweise	Klausur 90 min
Voraussetzungen	Kenntnisse und Fähigkeiten aus den Modulen Risk Assessment (SEC-V1) und Governance, Frameworks & Standards (SEC-V2)

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber

Studieninhalte

Zertifikat IT-Security Engineering

Security Design	
Lernziele	Die Studierenden lernen grundsätzliche Aspekte und Prinzipien von Sicherheitsentwürfen für Softwareanwendungen, -Systemen und IT-System Landschaften kennen und können diese gegenüber Sicherheitsanforderungen bewerten
Inhalt	▪ Die unterschiedlichen Perspektiven des Entwurfs von Anwendungen, Systemen und IT Landschaften bezüglich Ihrer Sicherheitseigenschaften werden exemplarisch betrachtet ▪ Es werden Netzwerks und Perimetersicherheitsbetrachtungen, Benutzerzugangsverwaltungs- und Berechtigungskonzepte und Entwürfe zur Systemsicherheits- und Serviceanbindungskonzepten (z.B. Cloud) vorgestellt

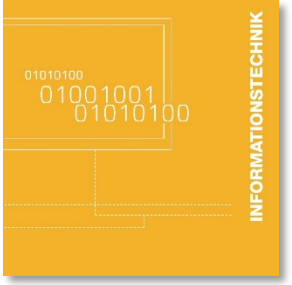
OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber

Studieninhalte

Zertifikat IT-Security Engineering

Security Application Development	
Vertiefung	SEC
Nummer	SEC-V4
Lehrveranstaltung	3 SU, 1 Ü
Modulverantwortlicher	Christian S. Fötinger, M.Sc.
Arbeitsbelastung	Es wird angenommen, dass durchschnittliche Studierende 75 Stunden Arbeitsaufwand benötigen, um sich die genannten Kenntnisse und Fähigkeiten anzueignen. Diese verteilen sich wie folgt: ▪ 45 Std. Präsenz in Lehrveranstaltungen und Übungen ▪ 15 Std. regelmäßige Nachbereitung des Lehrstoffes ▪ 45 Std. Erstellung von Übungsprogrammen und Programmlösungen ▪ 25 Std. Literaturstudium und freies Arbeiten ▪ 20 Std. Prüfungsvorbereitung Daraus ergeben sich 5 Leistungspunkte.
SWS / Leistungspunkte	4 SWS / 5 ECTS
Leistungsnachweise	Klausur 90 min
Voraussetzungen	Kenntnisse und Fähigkeiten aus den Modulen Risk Assessment (SEC-V1), Governance, Frameworks & Standards (SEC-V2) und Security Design (SEC-V3)

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber



Studieninhalte

Zertifikat IT-Security Engineering

Security Application Development

Lernziele	▪ Die Studierenden lernen Prinzipien, Verfahren und Werkzeuge kennen mit denen Sicherheitsaspekte von IT Anwendungen über den gesamten Softwarelebenszyklus berücksichtigt werden können ▪ Dabei soll Verständnis geschafft werden, welche Verantwortung die verschiedenen Rollen vom Kunden über den Product Owner, Tester bis zum Entwickler bei der Entwicklung sicherer Softwareanwendungen haben
Inhalt	▪ Prinzipien, Verfahren und Werkzeuge mit denen Sicherheitsaspekte von IT Anwendungen über den gesamten Softwarelebenszyklus berücksichtigt werden können ▪ Dokumentation von Sicherheitsanforderungen ▪ Überwachung der Umsetzung von Sicherheitsanforderungen ▪ Umsetzung von Sicherheitsanforderungen und Organisation der Behebung, oder Milderung von Sicherheitsrisiken

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber

Studieninhalte

Zertifikat IT-Security Engineering

Security Operations	
Vertiefung	SEC
Nummer	SEC-V5
Lehrveranstaltung	3 SU, 1 Ü
Modulverantwortlicher	Christian S. Fötinger, M.Sc.
Arbeitsbelastung	Es wird angenommen, dass durchschnittliche Studierende 75 Stunden Arbeitsaufwand benötigen, um sich die genannten Kenntnisse und Fähigkeiten anzueignen. Diese verteilen sich wie folgt: ▪ 45 Std. Präsenz in Lehrveranstaltungen und Übungen ▪ 15 Std. regelmäßige Nachbereitung des Lehrstoffes ▪ 45 Std. Erstellung von Übungsprogrammen und Programmlösungen ▪ 25 Std. Literaturstudium und freies Arbeiten ▪ 20 Std. Prüfungsvorbereitung Daraus ergeben sich 5 Leistungspunkte.
SWS / Leistungspunkte	4 SWS / 5 ECTS
Leistungsnachweise	Klausur 90 min
Voraussetzungen	Kenntnisse und Fähigkeiten aus den Modulen Risk Assessment (SEC-V1), Governance, Frameworks & Standards (SEC-V2), Security Design (SEC-V3) und Secure Application Development (SEC-V4))

Studieninhalte

Zertifikat IT-Security Engineering

Security Operations

Lernziele	▪ Die Studierenden lernen wie der sichere Betrieb von IT Systemen, -Systemverbünden und Anwendungen organisiert und überwacht werden kann ▪ Erkennen des Mehrwerts eines Sicherheitsinformationszentrums und entsprechender Werkzeuge
Inhalt	▪ Proaktive und reaktive Erkennung von Sicherheitsschwachstellen und deren Absicherung und Verwaltung ▪ Aktive Verteidigungsmaßnahmen und Verfahren zur Erkennung, Untersuchung und Bewertung von Sicherheitsereignissen ▪ Funktionsweise eines Sicherheitsinformationszentrums ▪ Werkzeuge zur Wiederherstellung von Systemen und Anwendung, der Archivierung und der Zugriffssicherung von Protokollen, sowie der Verwaltung von Schwachstelleninformationen und -Ereignissen

OPS_3010_INFO_Infomaterial M_FM Vers. , 18.03.2021, C.Schmidhuber