Qualifikationsziele
Master Cyber Security

Zentrum für Akademische Weiterbildung der Technischen Hochschule Deggendorf

Verfasser: Prof. Dr. Andreas Grzemba, Studiengangsleiter für den Masterstudiengang Cyber Security

Geschlechtsneutralität

Auf die Verwendung von Doppelformen oder anderen Kennzeichnungen weiblichen, männlichen und diversen Geschlechts wird weitgehend verzichtet, um die Lesbarkeit und Übersichtlichkeit zu wahren. Alle Bezeichnungen für die verschiedenen Gruppen von Hochschulangehörigen beziehen sich auf Angehörige aller Geschlechter der betreffenden Gruppen gleichermaßen.

Stand: 16.12.2020

Inhaltsverzeichnis

1 Ziele des Studiengangs

Die Studierenden besitzen nach Abschluss des berufsbegleitenden Masterstudienganges Cyber Security die Fähigkeit, Bedrohungen und Gefahren für individuelle Anwendungsfälle zu erkennen und zu formulieren, das resultierende Risiko zu analysieren sowie selbständig geeignete Sicherheitsstrategien zu erarbeiten und umzusetzen.

Weiter sind die Studierenden durch das vermittelte Wissen des berufsbegleitenden Masterstudienganges Cyber Security in der Lage, Sicherheitsvorfälle in den Bereich Industrial und Automotive zu erkennen und darzustellen, was sowohl bei forensischen Untersuchungen als auch beim Informationssicherheitsmanagement unerlässlich ist.

Durch heterogene Studiengruppen werden die Studierenden auf ihr späteres Arbeitsleben im Unternehmen vorbereitet.

2 Lernergebnisse des Studiengangs

Das akademische Weiterbildungsprogramm wird in fünf Semestern durchgeführt. Das erste Semester sieht die Vermittlung von Grundlagen des „Security Lifecycle Managements für Industrie und Automotive" vor. Die Studierenden werden es als ein Konzept zur nahtlosen Integration sämtlicher Informationen, die im Verlauf des Security-Lebenszyklus einer Anlage, eines Produktes oder eines Automobils anfallen, verstehen.

In den Modulen „Security Engineering I und II" werden Werkzeuge, Prozesse und Methoden für Entwurf, Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und Automotive behandelt, die befähigen, Security Engineering als ganzheitlichen Ansatz zu begreifen und zu bewerten.

Im Modul „Secure Product Development" werden den Studierenden die grundlegenden Standards und gesetzlichen Bestimmungen für den Schutz von Industrieanlagen vermittelt. Dazu erwerben die Studierenden Kompetenzen in Industrial Security Standards and Laws. Zudem erhalten die Studierenden Kompetenzen in Security Auditing. Ziel ist das Erfassen potentieller Sicherheitslücken unterschiedlicher Systeme. Dazu gehört die Evaluierung von Systemen in Bezug auf IT-Sicherheit.

Des Weiteren werden im zweiten Semester im Modul „Secure Operations and Maintenance" die wichtigen Methoden zum Betrieb und der Wartung von Automationsanlagen und IOT vermittelt. Es werden Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für die Industrieautomation vorgestellt. Insbesondere wird auf den Faktor Mensch und die Zugangskontrolle eingegangen. Zudem werden neue Entwicklungen aus der Forschung diskutiert.

Im dritten Semester erfolgt die Erstellung einer Projektarbeit zu einem Thema aus dem Fachgebiet Cyber Security. Diese soll den Studierenden die Fähigkeit vermitteln, komplexe wissenschaftlich-technische Probleme aus dem Bereich Cyber Security weitgehend selbstständig oder in kleinen Gruppen unter Anleitung eines kompetenten Hochschulwissenschaftlers zu bearbeiten. Dazu müssen die Studierenden ihr Vorgehen zeitlich und inhaltlich planen und strukturieren und die Ergebnisse in entsprechender Form dokumentieren.

Das vierte Semester vermittelt den Studierenden im Modul „Security Incident Management" Methoden, um den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Systemen und Industrieanlagen, in IOT und Automotive sowie hierzu vorbereitende Maßnahmen und Prozesse kennenzulernen. Diese umfassen organisatorische, rechtliche sowie technische Aufgabenstellungen.

Das Modul „Best Practise in Information Security Auditing" soll die Studierenden für mögliche Gefahren in der IT-Welt sensibilisieren, um das erlangte Wissen gezielt für geeignete Präventionsmaßnahmen einsetzen zu können. Dazu erwerben die Studierenden Kompetenzen in Security Auditing. Ziel ist das Erfassen potentieller Sicherheitslücken unterschiedlicher Systeme. Dazu gehört die Evaluierung von Systemen in Bezug auf IT-Sicherheit.

Zudem werden den Studierenden im Modul „Communication and Network Security" die wichtigen Methoden für die gesamten organisatorischen und technischen Prozesse für die Absicherung von Industrieanlagen vermittelt. Es werden angepasste Methoden für eine Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in Industrieanlagen sowie in IOT und hierzu vorbereitende Maßnahmen und Prozesse vorgestellt. Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können komplexe technische Protokolle analysieren und deren Schwachstellen erkennen sowie geeignete Absicherungsmaßnahmen ergreifen.

Im fünften Semester wird die Master-Thesis fertiggestellt und im Rahmen einer mündlichen Prüfung in Form eines Masterkolloquiums nochmals aufgegriffen und verteidigt.

3 Studienziele und Qualifikationsziele

Kenntnisse:

Die Absolventen besitzen umfangreiche ingenieurwissenschaftliche Kenntnisse in Cyber Security. Sie kennen die wesentlichen Begriffe und Methoden für die unterschiedlichen Bereiche. Im Einzelnen besitzen sie technische, sicherheitsrelevante und ingenieurwissenschaftliche Grundlagen sowie Inhalte zu der Ingenieurpraxis und der Produktentwicklung.

Sie haben Kenntnisse zu der organisatorischen Planung, Durchführung und Implementierung von Sicherheitskonzepten. Zudem verfügen sie über ein vertieftes Wissen im Security Engineering, dem Incident Management und dem Security Auditing. Sie sind vertraut mit weiterführenden kryptographischen Algorithmen und Protokollen sowie der forensischen Datenanalyse und dem Audit Reporting.

Die Absolventen haben ein gemeinsames Begriffsverständnis über Bedrohungen, Schwachstellen, Gegenmaßnahmen und verwandte Konzepte. Sie kennen die grundlegenden technischen Aspekte des multidisziplinären Security Engineerings. Darüber hinaus können die Absolventen komplexe technische Protokolle analysieren und deren Schwachstellen erkennen sowie geeignete Absicherungsmaßnahmen ergreifen.

Sie sind zu selbständiger wissenschaftlicher Arbeit und verantwortlichem Handeln in den jeweiligen Berufsfeldern befähigt. Zudem erkennen sie die Notwendigkeit der dauernden Weiterentwicklung mit sich verändernden Arbeits- und Lerninhalten.

Fähigkeiten: Die Absolventen sind in der Lage,

- Systeme in Bezug auf IT-Sicherheit zu evaluieren, wie das Erkennen von Schwachstellen in Applikationen und Betriebssystemen oder das Durchführen einer entsprechenden Sicherheitsbewertung nach aktuellen Normen.
- die wichtigsten Gefährdungen oder Bedrohungen für Industrial Control Systems einzuordnen und Standards der sicheren Produkt- und Anlagenentwicklung anzuwenden.
- komplexe technische Protokolle zu analysieren und deren Schwachstellen zu erkennen sowie geeignete Absicherungsmaßnahmen zu ergreifen.
- Bedrohungen und Gefahren für individuelle Anwendungsfälle zu erkennen und zu formulieren, das resultierende Risiko zu analysieren sowie selbständig geeignete Sicherheitsstrategien zu erarbeiten und umzusetzen.
- komplexe wissenschaftlich-technische Probleme aus dem Bereich Cyber Security selbstständig auf wissenschaftlicher Grundlage zu bearbeiten und zu lösen.

- Sicherheitsvorfälle im Bereich Industrial und Automotive zu erkennen und darzustellen, was sowohl bei forensischen Untersuchungen, als auch beim Informationssicherheitsmanagement unerlässlich ist.
- technische Standards, Gesetze und Verordnungen zu bewerten und auf komplexe technische Systeme anzuwenden.
- Security Technologien im Kontext von Industrie 4.0, bei kritischen Infrastrukturen und beim autonomen Fahren anzuwenden.

Kompetenzen: Die Absolventen haben die Kompetenz,

- das erworbene Wissen zu vertiefen und auf industrielle Anwendungen zu transferieren und sich somit zügig methodisch und systematisch in neue, unbekannte Aufgaben einzuarbeiten.
- durch den hohen Praxisbezug während des Studiums, die theoretischen Grundlagen unmittelbar in das berufliche Umfeld zu integrieren.
- komplexe Aufgabenstellungen zu erkennen und fachübergreifend, ganzheitlich und methodisch zu lösen.
- Methoden, Prozesse und Organisationsstrukturen basierend auf technischen Standards, Gesetzen und Verordnungen zu bewerten und zu überprüfen.
- einschlägige wissenschaftliche Methoden und neue Erkenntnisse der Wissenschaften auf Aufgabenstellungen in der Praxis anzuwenden.
- ihre Ideen und Ergebnisse logisch und überzeugend in mündlicher und schriftlicher Form zu kommunizieren und nach wissenschaftlichen Standards zu präsentieren.
- das Security Engineering auf komplexe technische Systeme anzuwenden und den Faktor Mensch im Kontext der Cyber Security zu bewerten.
- Bedrohungen, Schwachstellen, Gegenmaßnahmen und verwandte Konzepte für Industrial Control Systems und die Systematik wichtiger Publikationen zu kennen und einzuordnen.
- Sicherheitsstrategien zu erstellen sowie diese zu planen, durchzuführen und zu implementieren.

4 Lernergebnisse der Module / Modulziele / Zielematrix

Die einzelnen Module, ihre Detailziele und die von den Absolventen zu erwerbenden Kompetenzen sind in den Modulhandbüchern für den Masterstudiengang beschrieben. In der folgenden Tabelle wird der Zusammenhang zwischen den einzelnen Modulen und den im vorherigen Abschnitt beschriebenen Zielen im Masterstudiengang hergestellt.

Zielematrix der Module im Masterstudiengang Cyber Security

Modul	Ziele														
	Kenntnisse					Fähigkeiten					Kompetenzen				
	Wirtschaftswissenschaftlich-organisatorische GL	ingenieurwissenschaftliche Grundlagen und Methoden	Informationstechnologische Grundlagen und Methoden	Ingenieurspraxis	Überfachlich	Wirtschaftswissenschaftlich-organisatorische GL	ingenieurwissenschaftliche Grundlagen und Methoden	Informationstechnologische Grundlagen und Methoden	Ingenieurspraxis	Überfachlich	Wirtschaftswissenschaftlich-organisatorische GL	ingenieurwissenschaftliche Grundlagen und Methoden	Informationstechnologische Grundlagen und Methoden	Ingenieurspraxis	Überfachlich
Security Lifecycle Management	xx		xx			xx		xx			xx		xx		
Security Engineering I		xx	x	x			xx	x	x			xx	x	x	
Security Engineering II		xx	x	x			xx	x	x			xx	x	x	
Secure Operations and Maintenance			xx		xx			xx		xx			xx		x x
Project		x	x	xx	xx		x	x	xx	xx		x	x	xx	x x
Security Incident Management	xx		x	x		xx		x	x		xx		x	x	
Best Practise in Information Security Auditing		x	xx	xx			x	xx	xx			x	xx	xx	
Secure Product Development	x	x	x	xx		x	x	x	xx		x	x	x	xx	
Communication and Network Security		x	xx	x	xx		x	xx	x	xx		x	xx	x	x x
Thesis					xx					xx					x x

Legende: xx starker Bezug; x mittlerer Bezug