Masterstudiengang Cyber Security (M.Sc.) an der HDBW Start WS19/20

Kurzbeschreibung:

Das Thema Cyber Security ist für Unternehmen, Organisation, Regierungen und Personen von immer größerer Bedeutung. Viele Unternehmen sind auf der Suche nach Spezialisten, um ihre Informationen und Systeme vor Risiken, Bedrohungen und Krisen zu schützen. Cyber Security betrifft dabei nicht nur Computer oder das Internet. Sie umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik sowie Operational Technologies aus dem Bereich von Industrieanlagen sowie öffentlichen Versorgungsnetzen. Sie schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Die Abhängigkeit von multiplen, komplexen, interagierenden digitalen Systemen wächst von Tag zu Tag. Fahrzeuge, architektonische Infrastrukturen, Industriesteuerungen, Finanzflüsse und medizinische Geräte sind heute Teil der Cyber Domäne und daher vielfältigen Gefahren ausgesetzt. Die rasante Entwicklung in der Künstlichen Intelligenz führt dabei zu völlig neuen disruptiven Entwicklungen, die Unternehmen vor große Herausforderungen auch in der Cyber Security stellt.

Der Masterstudiengang Cyber Security ist ein anwendungsorientierter Studiengang, der sich mit Herausforderungen, Problemen und Lösungen der Cyber Sicherheit beschäftigt. Der Studiengang richtet sich an Personen, die die vielfältigen Aspekte der Cyber Security verstehen und anwenden möchten. Im Laufe des Studiums entwickeln sie ein klares Verständnis der Cyber-Bedrohungslandschaft sowie der Entwicklung von Cyber-Vorfällen. Sie werden die Schlüsseltechnologien kennen lernen und selbst umsetzen, die erforderlich sind, um Informationsinfrastrukturen in unterschiedlichen Szenarien vor Bedrohungen und Angriffen zu schützen. Sie lernen, wie sie die Auswirkungen eines Angriffs auf ein Unternehmen steuern und begrenzen können. Vor allem werden der Einsatz und die Auswirkungen von KI in Cyber Angriffen sowie Schutz und Abwehr behandelt und in praktischen Anwendung kennengelernt. In zwei unterschiedlichen Spezialisierungsrichtungen wird entweder der Bereich Technik oder aber Organisation und Management stärker vertieft.

Qualifikationsziele:

1. Die Studierenden kennen die unterschiedlichen System- und Netzwerkarchitekturen und können sie hinsichtlich ihrer Sicherheit und der Bedrohungspotentiale beurteilen.

2. Die Studierenden beherrschen die wesentlichen theoretischen Grundlagen aus dem Umfeld Verschlüsselung und deren praktischen Einsatz.

3. Die Studierenden kennen Methoden und Werkzeuge, mittels derer Angriffe auf die verschiedenen Systeme vorgenommen werden können.

4. Die Studierenden wenden Methoden und Werkzeuge zu Erkennung, Schutz und Abwehr von Angriffen auf verschiedenen Ebenen und Wegen an und kennen Vorgehensweisen zur Desaster Recovery.

5. Die Studierenden kennen die Bedeutung von Sicherheit im gesamten Lebenszyklus von Anwendungen und sind in der Lage, Cyber Security Anforderungen vom Entwurf bis End-of-Life umzusetzen.

6. Die Studierenden kennen die wesentlichen organisatorischen und rechtlichen Aspekte im nationalen und internationalen Kontext sowie die Anforderungen an Governance und Compliance, die im Umfeld Cyber Security relevant sind.

7. Die Studierenden lernen in den unterschiedlichen Modulen neueste Ansätze aus der Künstlichen Intelligenz und deren Anwendungsmöglichkeiten in der Cyber Security kennen. Sowohl im Schutz als auch im Angriff von Systemen, Netzwerken und Anwendungen sind KI Kenntnisse zunehmend von großer Bedeutung.

8. Die Studierenden haben ein anwendungsorientiertes Verständnis der aufgelisteten Aspekte und sind befähigt, diese als Mitarbeiter in verantwortender Position im Bereich Cyber Security technisch und organisatorisch selbständig umzusetzen.

9. In jeweils unterschiedlich angebotenen Modulen, aus denen zwei ausgewählt werden müssen, werden zusätzliche Kenntnisse zu Wirtschaftlichkeitsaspekten, Kommunikationsfähigkeiten, Projektmanagement oder weiteren vermittelt.

Voraussetzungen:

Bachelor Hochschulabschluss in Informatik, Wirtschaftsinformatik, Wirtschaftsingenieurwesen oder Elektro-/Informationstechnik oder eines vergleichbaren Fachs

Aufbau und Struktur des Studiengangs:

Der Masterstudiengang Cyber Security umfasst 90 ECTS Punkte bei einem Gesamtarbeitsaufwand (WL) von 2700 Stunden.

Einen Überblick über den Aufbau des Studiums in Vollzeit und Teilzeit geben die folgenden beiden Abbildungen:

Master CyberSecurity Vollzeit					
1. Semester					
Grundlagen Cyber Security - Introduction to Cyber Security	Kryptographie - Cryptography	Computersysteme und Netzwerke - Systems and Networks	Systemanalyse und Härtung - System Auditing and Hardening	Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	WPF: Python und Go, Human Factors in CySe, Ethik, Soft Skills (Projektmanagement, Story Telling, Kommunikation)- Python and Go for Security, Human Factors in CySe, Ethics, Soft Skills
2. Semester					
Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	Seminar: aktuelle Themen der Cyber Security	Reifegradmodelle - Security Maturity	Security Governance and Compliance	Sicherheitsmanagement - Security Manangement
			Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics	System- und Netzwerksicherheit - System and Network Security	Methoden der Künstlichen Intelligenz (KI) - AI Methods
3. Semester					
Incident Management and Disaster Recovery	Requirements Engineering and Threat Modelling	Masterthesis			

Legende
Modul für alle Teilnehmer
Schwerpunktmodul Technik
Schwerpunktmodul Management
WPF: 2 aus den angebotenen Modulen

Abbildung 1 Studiengang im Vollzeitmodell

Master CyberSecurity Teilzeit			
1. Semester			
Grundlagen Cyber Security - Introduction to Cyber Security	Kryptographie - Cryptography	Computersysteme und Netzwerke - Systems and Networks	Systemanalyse und Härtung - System Auditing and Hardening
2. Semester			
Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	Reifegradmodelle - Security Maturity	Security Governance and Compliance	Sicherheitsmanagement - Security Manangement
	Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics	System- und Netzwerksicherheit - System and Network Security	Methoden der Künstlichen Intelligenz (KI) - AI Methods
3. Semester			
Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	Incident Management and Disaster Recovery	Requirements Engineering and Threat Modelling	WPF: Python und Go, Human Factors in CySe, Ethik, Soft Skills (Projektmanagement, Story Telling, Kommunikation)- Python and Go for Security, Human Factors in CySe, Ethics, Soft Skills
4 Semester			
Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	Seminar: aktuelle Themen der Cyber Security		
5. Semester			
Masterthesis			

Legende
Modul für alle Teilnehmer
Schwerpunktmodul Technik
Schwerpunktmodul Management
WPF: 2 aus den angebotenen Modulen

Abbildung 2 Studiengang im Teilzeitmodell