

Qualifikationsziele

Bachelorstudiengang Unternehmens- und IT-Sicherheit

Fachliche Qualifikationsziele:

Um die Absolventen des Studiengangs Unternehmens- und IT-Sicherheit für die vielfältigen Aufgaben in ihren späteren Berufsfeldern zu rüsten, werden gefragte Qualifikationen und Kernkompetenzen in verschiedenen Gebieten vermittelt und miteinander verknüpft. Den Studierenden ein anwendungsbezogenes, herstellerunabhängiges und produktübergreifendes Know-how in nahezu allem Bereichen der IT-, Daten- und Prozesssicherheit, IT-Schutzmechanismen, sowie deren Integration in den Unternehmensworkflow vermittelt.

Methodische Qualifikationsziele:

Die im Studienverlauf erworbenen fachlichen Qualifikationen ermöglichen es den Studierenden im späteren beruflichen Einsatz, branchenunabhängig die sicherheitsrelevanten Erfordernisse für ein Unternehmen zu erkennen und anzuwenden. Zudem werden die wesentlichen Aspekte aus Technik, Management und Recht während des Studiums in praktischen Übungen angewendet und vertieft.

Überfachliche Qualifikationsziele:

Die übergreifenden Bildungsziele wie die Befähigung zum wissenschaftlichen Arbeiten, die Befähigung, eine qualifizierte Erwerbstätigkeit aufzunehmen, die Befähigung zum zivilgesellschaftlichen Engagement sowie die Persönlichkeitsentwicklung ist im Studiengang sichergestellt. Den Anforderungen des Qualifikationsrahmens für deutsche Hochschulabschlüsse sowie der länderspezifischen Strukturvorgaben wird entsprochen. Dies ist bereits von der Gutachterkommission der Erstakkreditierung am 21.09. 2010 so festgestellt worden. Die Kommission hat dabei nicht nur den Studienaufbau als stimmig bewertet, sondern auch konstatiert, dass mit dem Studiengangskonzept die definierten Qualifikations- bzw. Bildungsziele erreicht werden können, da Fachwissen und fachübergreifendes Wissen ebenso wie methodische und generische Kompetenzen vermittelt werden.

Mit Sicherheit Karriere machen – ist ein Versprechen, welches der Studiengang Unternehmens- und IT-Sicherheit vollumfänglich zu realisieren vermag!

Der Bachelor-Studiengang Unternehmens- und IT-Sicherheit erreicht folgende wesentliche Qualifikationsziele, welche sich sowohl in fachliche und methodische als auch überfachliche Kompetenzen gliedern:

Qualifikationsziel		Absolventen des Bachelor-Studiengangs Unternehmens- und IT-Sicherheit
K1	Allgemeine und technische IT-Sicherheit	... verstehen die Grundlagen, Ziele, Konzepte, Modelle und Mechanismen moderner IT-Sicherheit und können diese in konkreten Situationen zur Anwendung bringen, wobei sie in der Lage sind, Sicherheitsrisiken sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen, was sie zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt;
K2	Organisatorische Sicherheit	... sind in der Lage, das erforderliche IT-Sicherheitsniveau für unterschiedliche Bereiche eines Unternehmens festzustellen, die geeigneten Sicherheitsstrategien zu bestimmen und die daraus resultierenden Sicherheitsmaßnahmen einzuleiten;
K3	Sicherer Entwurf und Entwicklung	... sind in der Lage, Systeme sowie Anwendungen zu analysieren, zu entwerfen, zu entwickeln und zu pflegen, so dass sie den heutigen Maßstäben an die Sicherheit gerecht werden
K4	Gesellschaft und Sicherheit	... sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst;

K5	Fach- und Methodenkompetenz der Informatik	... verstehen grundlegende und aktuelle technische Konzepte der Informatik und können diese hinterfragen, bewerten und anwenden, können ihr Wissen und Verstehen eigenständig ergänzen und erweitern und haben eine Fach- und Methodenkompetenz mit tiefgehendem Informatikwissen (Algorithmen, Programmierung, Softwareentwicklung, Betriebssysteme und Netzwerke, verteilte Systeme, IT-Security, etc) erworben, die ihnen ermöglicht, gängige technische und mathematische Konzepte zu beherrschen, die sie zum Lösen informationstechnischer Fragestellungen befähigen;
K6	Managementkompetenz	... können grundlegende Fragestellungen des Unternehmens erkennen und selbständig Fakten, Wissen und wirtschaftswissenschaftliche Konzepte bezüglich der unternehmerischen Strategie, Corporate Governance, Organisation, Compliance und Sicherheitsstandards für eine Problemlösung heranziehen, wobei sie in der Lage sind, komplexere Sachverhalte in Bezug auf Wirtschafts- und Cyberkriminalität sowie Buchhaltung und Kostenrechnung aufzubrechen, um neues anwendungsbezogenes Wissen zu generieren;
K7	Formale, technische und mathematische Kompetenzen	... beherrschen gängige technische und mathematische Konzepte, die sie zum Lösen informationstechnischer und IT-Sicherheitsrelevanter Fragestellungen befähigen;
K8	Analyse-Kompetenzen	... sind in der Lage, basierend auf Ihrer Fachkompetenz IT-Sicherheit und den algorithmischen sowie mathematischen Kompetenzen Anforderungen und Systeme zu analysieren und zu bewerten, um darauf aufbauend komplexe Bewertungs- und Anwendungskonzepte zu entwickeln und können dabei die Komplexität, Machbarkeit, Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen;
K9	Soziale Kompetenzen und Persönlichkeitsbildung	... sind in der Lage ihr Wissen und Verstehen zu bewerten, in das technische, wirtschaftliche und soziale Umfeld einzuordnen und zu vermitteln und dabei Informationen, Ideen, Probleme und Lösungen nachvollziehbar darzustellen;

Modul	Name	Qualifikationsziele / Kompetenzen								
		K1	K2	K3	K4	K5	K6	K7	K8	K9
UNITS-01	Grundlagen der Mathematik							x	x	
UNITS-02	Einführung in die IT-Security	x	x		x	x		x	x	x
UNITS-03	Computernetze			x		x		x	x	
UNITS-04	Programmierung	x		x		x		x	x	
UNITS-05	Betriebswirtschaft		x		x		x		x	
UNITS-06	Mathematik und Kryptografie							x	x	
UNITS-07	Software Engineering			x		x			x	
UNITS-08	Skripting und Hacking	x		x		x		x	x	
UNITS-09	Rechnerarchitektur und Betriebssysteme	x	x			x				
UNITS-10	Sicherheitsmanagement & Rechnungskreisläufe	x	x				x	x		
UNITS-11	Algorithmen und Datenstrukturen		x			x		x		
UNITS-12	Interaktive verteilte Systeme	x	x			x				
UNITS-13	Datenbanken	x		x		x				
UNITS-14	Sicherheit und Unternehmenskultur		x				x			
UNITS-15	Recht				x					x
UNITS-30	Sicherheit in Webapplikationen	x		x		x				
UNITS-31	Netzwerk-Sicherheit	x		x		x				x
UNITS-32	Sicherheitsmanagement und Unternehmensprozesse		x				x			x

UNITS-33	E-Business		x		x	x				
UNITS-34	Unternehmenspraxis	x	x	x		x	x		x	x
UNITS-35	Sicherheits- und Risikomanagement		x				x		x	
UNITS-36	Praxisarbeit IT-Sicherheit	x	x			x	x		x	x
UNITS-37	Projektarbeit	x	x	x		x	x			x
UNITS-38	Computer-Forensik	x			x	x		x	x	
UNITS-39	Theorie der IT-Sicherheit	x			x	x		x		
UNITS-40	International Security Trends	x		x	x		x		x	x
UNITS-41	Bachelorarbeit	x	x	x	x	x	x	x	x	x
UNITS-61	Reverse Engineering	x		x		x		x		
UNITS-62	Penetration Testing	x	x			x		x	x	
UNITS-63	Verlässliche verteilte Systeme	x		x		x		x	x	
UNITS-64	Prävention und Krisenmanagement		x		x		x		x	
UNITS-80	Querschnittskompetenz						x			x