

Modul / Lehrveranstaltungen	Typ	Semester / SWS / ECTS*					
		1	2	3	4	5	6

Technische Grundlagen	Ein wesentlicher Bestandteil dieses Moduls ist es, die notwendigen Programmierkenntnisse zu vermitteln, wobei der Schwerpunkt auf der sicherheitsrelevanten Aufgabe liegt, einen robusten Code von hoher Qualität zu entwickeln. Ein weiterer wichtiger Teil dieses Moduls sind die mathematischen Grundlagen, die die Basis für die Kryptografie und anderer Bereiche der Sicherheitsinformatik bilden.							
	Grundzüge der diskreten Mathematik	VO	3/4					
	Grundzüge der diskreten Mathematik	UE	2/3					
	Programmieren 1	VO	2/2					
	Programmieren 1	UE	2/3					
	Programmieren 2	VO		2/2				
	Programmieren 2	UE		2/3				
	Programmieren 3	ILV			2/2			

Netzwerktechnik	Netzwerke – Grundlagen: Beschäftigung mit verschiedenen Modellen, Netztopologien und den entsprechenden Protokollen. Dabei werden im 1. Semester TCP/IP und Ethernet schwerpunktmäßig behandelt, im 2. Semester stehen die Applikationsprotokolle auf dem Programm. Sehr viel Zeit wird auch für die Protokollanalyse im Labor mit den entsprechenden Tools aufgewendet, da dies grundlegendes Wissen für die Analyse von Sicherheitslücken und Angriffspotenzialen darstellt.							
	Einführung Netzwerke und verteilte Systeme	ILV	4/5					
	Applikationsprotokolle u. Protokollanalyse	ILV		3/4				
	Aktive Komponenten	ILV		3/5				
	Network Security: Hier werden die Grundlagen für die Berufsfelder NetzwerkadministratorIn bzw. Security-ArchitektIn gelegt. Die verschiedenen Konzepte der Sicherheitskomponenten und die verwendeten Protokolle werden besprochen und in entsprechenden Übungen nachgestellt. Übergreifend auf drahtgebundene (LAN) und drahtlose (WLAN) Zugangstechnologien wird die zentrale Authentifizierung von Komponenten im Netzwerk über 802.1x – basierend auf PEAP und EAP-TLS, im Zusammenspiel mit aktuellen RADIUS Servern wie zB Microsoft NPS, im 4. Semester gelehrt.							
	Netzwerk Sicherheitskomponenten	VO			1/1			
	Netzwerk Sicherheitskomponenten	LAB			2/3			
Secure Networks	ILV				4/5			

IT Betrieb	Betriebssysteme: Der Schwerpunkt der Grundlagen beim IT-Betrieb liegt im Verstehen von Zweck und Aufbau von Betriebssystemen sowie deren Server-Funktionalitäten. Wissen über die Prozessverwaltung, die Prozess-Synchronisation sowie die Speicherverwaltung und die Einbindung der Peripherie auf verschiedenen Plattformen (Windows, Unix), eignen sich die Studierenden sowohl theoretisch als auch praktisch in diesem Modul an. Außerdem wird bereits im Anfangsstadium ein Schwerpunkt auf die entsprechenden Sicherheitskonzepte und die Absicherung der Systeme gelegt.							
	Unix und Windows als Client/Server Betriebssysteme	ILV	5/8					
	Betriebssystem - Hardening	ILV		4/7				
	Sicherheit von heterogenen Rechnernetzen	ILV			5/8			
	Betrieb vernetzter Systeme: Die für den/die SicherheitsmanagerIn notwendigen Kompetenzen im Bereich des sicheren Betriebs von großen netzwerkbasierenden Applikations-Frameworks, der sicherheitskritischen Anwendungen sowie weit verbreiteten Angriffstechniken, werden im Modul „Sicherer Betrieb vernetzter Systeme“ vermittelt. Im 6. Semester lernen die Studierenden im Rahmen von „Web- und Applikationssicherheit“ theoretisch und praktisch Sicherheits-schwachstellen durch schlechte oder fehlerhafte Programmierung kennen. In der LV „Penetration Testing“ wird entsprechendes Know How zur manuellen und automatisierten Suche von Schwachstellen in Systemen vermittelt.							
	Datenbanksysteme	ILV				3/4		
	Betriebssysteme Internals	ILV				4/5		
	Web- und Applikationssicherheit	ILV						2/3
	Penetration Testing	ILV						2/3
Business-Continuity und Disaster-Recovery	UE						2/2	

Modul / Lehrveranstaltungen	Typ	Semester / SWS / ECTS					
		1	2	3	4	5	6

Sicherheits- technologien	Kryptografie: Dieses Modul gibt einen Überblick über die kryptografischen Methoden und Werkzeuge sowie Authentifizierungsmethoden. Ziel ist es dabei, den Studierenden das grundlegende Rüstzeug und das Verständnis für diese Materie zu vermitteln. Das Verstehen der kryptografischen Methoden und Werkzeuge schult das analytische Denken und bildet die entsprechenden Grundlagen für das Verständnis der Sicherheitseigenschaften (Sicherheitsdienste) Vertraulichkeit, Authentizität, Integrität und Verbindlichkeit. Hash-Methoden, PKI, Kryptoanalyse und Kryptostandards sind nur einige Beispiele, die in diesem Modul gelehrt werden.						
	Grundlagen der Kryptografie	VO		2/3			
	Grundlagen der Kryptografie	UE		2/3			
	Identifikation und Authentifikation	ILV			2/2		
	Hardwaretoken	ILV				2/3	

Sicherheitsmanagement	Wirtschaft und Recht: Vermittlung wichtiger Kenntnisse über grundlegende Inhalte im Bereich Rechtswissenschaften, Betriebswirtschaft (wie beispielsweise Kostenrechnung, Buchhaltung). Weiters werden die wesentlichen Aufgaben der Unternehmensführung (Zielsetzung, Planung, Organisation und Kontrolle) praxisnah dargestellt. In diesem Zusammenhang wird auch auf die Wechselwirkung zwischen Persönlichkeitsrechten (Datenschutz) und ihre Gewährleistung durch technische und organisatorische Maßnahmen eingegangen.						
	Teamtraining	ILV	1/11				
	Rechtliche Grundlagen	VO	2/2				
	Ethik	VO		1/11			
	Angewandte BWL	ILV				3/3	
	Outsourcing Modelle und Awareness	ILV				2/3	
	Sicherheitsorganisation und -strategie: Die Studierenden erhalten detaillierte Kenntnisse über Normen, Standards, Richtlinien und Regelungen im Umfeld der Informationssicherheit sowie die Fähigkeit, diese Kenntnisse in der Praxis anzuwenden. Ein besonderer Schwerpunkt liegt dabei auf der ISO270xx Serie, dem Grundschriftbuch, dem österreichischen Sicherheitshandbuch sowie ITIL v3 sowie ISO20000. Weiters wird den Studierenden in den Lehrveranstaltungen „Risikomanagement“ und „Business Continuity Management“ das entsprechende Rüstzeug mitgegeben, um Security-Management Systeme erfolgreich an internationale und nationale Standards auszurichten und in Unternehmen zu etablieren.						
	Sicherheitsnormen und Standards	ILV			4/5		
	IT Prozesse nach ITIL	ILV			2/3		
	Business Continuity Management	ILV					2/3
	Audit und Revision	ILV					1/11
	Risikomanagement	ILV					2/4

Arbeitstechniken & Sprachen	Arbeitstechnik: Der Bachelorstudiengang IT Security eröffnet den AbsolventInnen die Möglichkeit, Masterstudiengänge zu belegen und damit auch eine Berufstätigkeit an Hochschulen bzw. im wissenschaftlichen Bereich anzustreben. Deshalb ist es besonders wichtig, dass die Studierenden rechtzeitig auf das wissenschaftliche Arbeiten vorbereitet werden.						
	Methoden des wiss. Arbeiten und Bachelorarbeit	ILV				2/5	
	Projektmanagement	ILV				1/2	
	Fächerübergreifende Projektarbeit	PR					1/5
	Bachelorseminar mit Bachelorarbeit 2	SE					2/8
	Sprachen: Die beiden ersten Semester dienen zur Festigung der allgemeinen Sprachkompetenz mit Schwerpunkt auf der kommunikativen Kompetenz. Im 3. Semester müssen die Studierenden eine Präsentation auf Englisch erstellen, wobei sowohl die Sprachkompetenz als auch die Präsentationstechnik bewertet wird.						
	Englisch 1	ILV	2/2				
	Englisch 2	ILV		2/2			
Englisch 3	ILV			2/2			

* SWS: Semesterwochenstunden, ECTS: European Credit Transfer System – Maß für den gesamten Arbeitsaufwand für durchschnittliche Studierende, um eine Lehrveranstaltung positiv zu absolvieren. Ein Leistungspunkt (oder Credit Point) steht für 25 Stunden Studieren (Präsenzzeiten, Selbststudium, Prüfungen etc.). Vorlesung: VO, Seminar: SE, Integrierte Lehrveranstaltung: ILV, Übung: UE, Projektarbeit: PA, Laborübung: LAB, Fallstudie: FS;