Zürcher Hochschule
für Angewandte Wissenschaften

School of
Management and Law

Gültig für 2023.FS

Modulbezeichnung: IT-Security		
Modulkürzel	w.BA.XX.3ITS-WIN.XX	
Beschreibung des Moduls	Dieser Kurs vermittelt das notwendige Grundlagenwissen zu Themen der Informations- und Cybersicherheit. Dazu gehört initial auch eine fundierte Einführung in Computernetze. Beginnend mit der Kommunikation in Switched-Ethernet-Netzen und den verschiedenen Protokollen und Schichten (TCP/IP) schauen wir uns auch grundlegende Dienste und Architekturen im Internet an. Ausgestattet mit diesen Grundlagen bauen wir gemeinsam ein Verständnis von realen Bedrohungen und Verwundbarkeiten moderner IT-Infrastrukturen auf, lernen diese zu bewerten und geeignete Schutzkonzepte zu evaluieren. Neben Konzepten zum Schutz, wird auch notwendiges Wissen über die Erkennung von Vorfällen und das Aufarbeiten bereits erfolgter Angriffe vermittelt. Parallel zu den Vorlesungen findet praktischer Übungsbetrieb statt in welchem alle Themen dann praktisch angewendet werden. Dabei arbeiten wir vor allem mit virtualisierten/simulierten Umgebungen.	
Studiengang und Vertiefungsrichtung	§ Wirtschaftsinformatik - Vertiefung in Business Information Systems § Wirtschaftsinformatik - Vertiefung in Data Science	
Rechtliche Grundlagen	Studienordnung BSc vom 29.01.2009 für die Bachelorstudiengänge Betriebsökonomie, International Management, Wirtschaftsinformatik, Wirtschaftsrecht und Angewandtes Recht, erstmals beschlossen am 12.05.2009	
Modulkategorie	**Modultyp:** Pflichtmodul	**Studienabschnitt:** Assessment
ECTS	6	
Verantwortliche OE	W Institut für Wirtschaftsinformatik	
Modulverantwortung	Peter Heinrich (heip)	
Modulverantwortung Stellvertretung	Christian Weber (weei)	
Spezifische Vorkenntnisse	Keine	
Beitrag des Moduls für Learning Goals des Studiengangs (durch das Modul betroffene)	§ Fachkompetenz § Methodenkompetenz § Sozialkompetenz § Selbstkompetenz	
Beitrag des Moduls für Learning Objectives des Studiengangs	Fachkompetenz § Theorie- & Praxisrelevante Fachinhalte wissen & verstehen § Theorie- & Praxisrelevante Fachinhalte anwenden, analysieren und verknüpfen § Theorie- & Praxisrelevante Fachinhalte evaluieren Methodenkompetenz § Problemlösung & Kritisches Denken § Arbeitsmethoden, -techniken & -verfahren § Nutzung von Informationen § Kreativität & Innovation Sozialkompetenz § Mündliche Kommunikation Selbstkompetenz § Ethische & Soziale Verantwortung	
Lernziele des Moduls	Die Studierenden... § verstehen, wie Computernetze aufgebaut sind und können Kommunikationsvorgänge darin nachvollziehen. § können selbst kleine Computernetze (z.B. Heimnetz oder kleines KMU) sicher konfigurieren. § verstehen konzeptuell die im Internet angebotenen Dienste (HTTP, DNS, MAIL) sowie typische Infrastrukturdienste (z.B. DHCP/BootP), die auf den Standardprotokollen (ARP, IP, TCP, UDP) aufbauen. § können in grösseren Netzen IP-Routing und dazugehörige Konzepte (z.B. Weiterleitung, Filterung und NAPTv4) verstehen. § kennen wichtige Security-Threats und können diese im Kontext eines Unternehmens bewerten. § können für eine überschaubare Umgebung ein Schutz- und Recovery-Konzept vorschlagen. § haben ein Grundverständnis von Kryptographieverfahren, deren Algorithmen und Anwendungsgebieten. § können am Markt angebotene "Sicherheitsprodukte" in Bezug auf die Schutzwirkung bewerten und konkret am Beispiel eines spezifischen Unternehmens eine Bewertung dieser vornehmen.	

Inhalte des Moduls	§ OSI- TCP/IP-Model / Layer_1_2_PHY_MAC_Gigabit_Switched_Ethernet § Layer_3_Network_IPv4_IPv6_Addressing_Routing_CIDR § Layer_4_Transport_TCP_UDP_ICMP § Layer_5-7_Applications_DNS_DHCP_HTTP_SMTP § Computer Network Security Fundamentals § Security Threats / Vulnerabilities / Hackers § Security Assessment, Analysis and Assurance § Disaster Management § Cryptography § Access Control, Autorization and Authentication § Firewalling § Intrusion Detection / Forensics / Virus & Content Filtering
Verknüpfung zu anderen Modulen	-
Unterrichtsmethoden	§ Lehrvortrag § Lehrgespräch § Anwendungsaufgaben § Fallstudien § Übungen § Problemorientierter Unterricht **Eingesetzte Sozialformen:** Einzelarbeit
Digitale Lernressourcen	§ Übungs- und Anwendungsaufgaben (inkl. Lösungen) § (Multiple-Choice)-Tests

Unterrichtsgliederung	**Kontaktstudium**	**Begleitetes Selbststudium**	**Autonomes Selbststudium**
Grossklasse	28 h	12 h	
Kleinklasse	28 h	56 h	
Gruppenunterricht	-	-	
Praktikum	-	-	
Seminar	-	-	
Total	**56 h**	**68 h**	**56 h**

Leistungsnachweise

Modulendprüfung	**Form**	**Dauer (Min.)**	**Gewichtung**
Schriftliche Prüfung	open book	90	100,00 %
Hilfsmittel	kein Taschenrechner	mit Diktionär	

Andere	**Bewertung**	**Dauer (Min.)**	**Gewichtung**
12 x Lese-Tests zu Stundenbeginn (Grossklasse); mind. 6 müssen davon ein "PASS" erreichen.	Pass/Fail	5	-

Präsenzverpflichtung im Kontaktstudium	Zwingende Präsenzzeit: Andere An jedem Grossklassentermin wird es eingangs einen 5-Minuten Moodle-Multiple-Choice-Test geben, der die Erfüllung der Reading-Assignments überprüft. Dieser kann ausschliesslich zur jeweiligen Zeit durchgeführt werden. Eine Vor-Ort-Präsenz wird nicht verlangt, der Test kann in diesem Zeitfenster (ausschliesslich zu dem Termin in dem man auch zu einer bestimmten Grossklasse zugeteilt ist) auch remote durchgeführt werden.
Unterrichts- und Prüfungssprache	Deutsch
Pflichtliteratur	§ Baun, C. (2019). Computer Networks / Computernetze. Wiesbaden: Springer Vieweg. ISBN 978-3-658-26356-0. Im ZHAW-Netz/VPN kostenlos verfügbar: https://link.springer.com/book/10.1007/978-3-658-26356-0. § Kizza, J. (2020). Guide to Computer Network Security. Cham: Springer. ISBN 978-3-030-38141-7. Im ZHAW-Netz/VPN kostenlos verfügbar: https://link.springer.com/book/10.1007/978-3-030-38141-7.
Ergänzende Literatur	§ van Oorschot, P. (2020). Computer Security and the Internet. Cham: Springer. ISBN 978-3-030-33649-3. Im ZHAW-Netz/VPN kostenlos verfügbar: https://link.springer.com/book/10.1007/978-3-030-33649-3. § Al-Omari, Q. (2018). Practical Information Security. Cham: Springer. ISBN 978-3-319-72119-4. Im ZHAW-Netz/VPN kostenlos verfügbar: https://link.springer.com/book/10.1007/978-3-319-72119-4.
Bemerkungen	-