Syllabus

Kursbeschreibung

Titel der Lehrveranstaltung	Management of System Security and Networks
Code der Lehrveranstaltung	76437
Zusätzlicher Titel der Lehrveranstaltung	
Wissenschaftlich-disziplinärer Bereich	IINF-05/A
Sprache	Italienisch
Studiengang	Bachelor in Wirtschaftsinformatik
Andere Studiengänge (gem. Lehrveranstaltung)	
Dozenten/Dozentinnen	Prof. Fabrizio Maria Maggi, maggi@inf.unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/41895
Wissensch. Mitarbeiter/Mitarbeiterin	
Semester	Erstes Semester
Studienjahr/e	2
KP	6
Vorlesungsstunden	40
Laboratoriumsstunden	20
Stunden für individuelles Studium	90
Vorgesehene Sprechzeiten	18
Inhaltsangabe	- Key concepts of system security and networked systems, threats and data security - Basic mechanisms of cryptography - Software security - Web applications security - Security infrastructures and certificates - Network security

	- Risk management
Themen der Lehrveranstaltung	The course introduces the fundamental concepts related to the security of computer systems and networks, illustrating the main threats and strategies to protect data, applications, and infrastructures. The instruction begins with an overview of the key concepts in system and network security, highlighting the principles of confidentiality, integrity, and availability of information, as well as the concepts of authentication, authorization, and accountability. The course also presents the variety of cyber threats, including viruses, worms, trojans, ransomware, and spyware, and explains how these can compromise the security of data and systems. Subsequently, the course delves into the basic mechanisms of cryptography. It explains the differences between symmetric and asymmetric cryptography, methods for key management, and the use of digital signatures to ensure data authenticity and integrity. The concept of hashing is also addressed, including the properties of hash functions and the issues related to collisions. Additionally, the course describes methods for secure key exchange and practical applications of digital certificates. Another focus of the course is web application security. The most common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), are analyzed, explaining how attackers can exploit them. Software security is discussed, including issues related to buffer overflows, and the main strategies to prevent such vulnerabilities are illustrated. The course also covers the architectures of security devices and related infrastructures. Firewalls, intrusion detection and prevention systems (IDS/IPS), proxies, and other devices are described. The role of public key infrastructures (PKI) and digital certificates is examined in depth, as they are essential for ensuring authenticity in digital communication. A specific module is dedicated to network security, with particular attention to secure communication protocols, access control, network segmentation, and techniques for protecting against interception. Threats such as ARP poisoning, DNS poisoning, and

	man-in-the-middle attacks are illustrated, along with countermeasures to mitigate them. Finally, the course focuses on risk management and resilience strategies. Topics include risk assessment, threat analysis, the definition of security policies, and mitigation plans. Concepts such as redundancy, fault tolerance, backup systems, and disaster recovery are explored in detail.
Stichwörter	Cryptography, Web Application Security, Software Security, Network Security, Risk Management
Empfohlene Voraussetzungen	Students should be familiar with basic programming concepts, data structures and algorithms. These prerequisites are covered in any Bachelor degree in Informatics and Management of Digital Business.
Propädeutische Lehrveranstaltungen	
Unterrichtsform	Frontal classroom lecture and lab sessions.
Anwesenheitspflicht	Attendance is not compulsory but recommended. Non-attending students have to contact the lecturer at the start of the course to agree on the modalities of the independent study. Exam modalities for non-attending students are the same as for attending students.
Spezifische Bildungsziele und erwartete Lernergebnisse	The course belongs to the type "caratterizzante - informatica". The main aim of this exam is to provide an introduction to the field of information security. The students learn about the technical as well as the management side of security in information systems. They acquire knowledge about fundamental principles of security and also about practical approaches to securing information systems. Knowledge and understanding: - D1.7 - Know the main concepts of computer networks and security in distributed systems. Applying knowledge and understanding: - D2.3 - Ability to analyse business problems and to develop proposals for solutions with the help of IT tools. - D2.4 - Ability to formalise and to analyse procedures and operational processes, to recognise and use optimisation

	potentials. - D2.10 - IT infrastructure and project management capabilities. Making judgments - D3.2 - Be able to work independently according to your level of knowledge and understanding, also taking responsibility for development projects or IT consulting. Learning skills - D5.3 - Ability to follow rapid technological developments and to learn about innovative aspects of the latest generation of information technology and systems.
Spezifisches Bildungsziel und erwartete Lernergebnisse (zusätzliche Informationen)	
Art der Prüfung	- Project work to test knowledge application skills - Oral exam with verification questions and discussion of the project
Bewertungskriterien	Assessment 1: project work (30%) Assessment 2: oral exam (70%) Relevant for assessment 1: skills in applying knowledge in a practical setting, ability to summarize in your own words, ability to explain things balancing conciseness and completeness. Relevant for assessment 2: clarity of answers, ability to recall principles and methods used in information security, skill in applying knowledge about information security.
Pflichtliteratur	CompTIA Security+ Guide to Network Security Fundamentals 6thEdition, Mark Ciampa ISBN 978-1337288781 Material provided in the form of slides and scientific papers provided by the teacher.
Weiterführende Literatur	Computer & Internet Security: A Hands-on Approach 3rd Edition ISBN: 978-17330039-4-0

	Computer Security: A Hands-on Approach 3rd Edition ISBN: 978-17330039-5-7 Internet Security: A Hands-on Approach 3rd Edition ISBN: 978-17330039-6-4
Weitere Informationen	Software used: Provided by teacher during lectures/lab sessions
Ziele für nachhaltige Entwicklung (SDGs)	Hochwertige Bildung