COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security in cloud systems [S1Cybez1>BSCh]

Course

Field of study
Cybersecurity

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
24

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
16

Number of credit points

4,00

Coordinators

dr inż. Michał Weissenberg
michal.weissenberg@put.poznan.pl

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

Lecturers

Prerequisites

A student starting this course should have basic knowledge of telecommunication networks, operating systems, cloud systems, and basic programming skills. They should also have the ability to acquire information from specified sources. The student should demonstrate qualities such as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for others, and readiness to work in a team.

Course objective

• Providing students with theoretical foundations regarding cloud systems. • Introducing students to theoretical information on the security of cloud system infrastructure. • Familiarizing students with basic information on cloud security management and risk assessment. • Introducing students to fundamental concepts of data security in cloud systems. • Providing students with basic knowledge of cloud security operations, identity management, and access control.

Course-related learning outcomes

Knowledge:
• The student has advanced and in-depth knowledge of network devices used in cloud systems. [K2_W07]
• The student understands the methodology of designing complex IT systems, knows hardware description languages, and is familiar with computer tools for designing and simulating cloud systems. [K2_W14]
• The student knows and understands the threats faced by modern civilization, which extensively relies on digital services, particularly cloud services. [K2_W22]

Skills:
• The student is able to acquire information from literature, databases, and other sources; integrate obtained information, interpret and critically evaluate it, as well as draw conclusions and formulate well-justified opinions. [K2_U01]
• The student can propose improvements or alternative solutions for existing design solutions and telecommunication systems in the field of cloud computing. [K2_U09]
• The student is able to assess the applicability and feasibility of using new achievements in techniques and design methods for developing and manufacturing telecommunication systems that incorporate innovative cloud computing solutions. [K2_U11]

Social competences:
• The student is prepared to recognize the importance of knowledge in solving cognitive and practical problems and to critically evaluate received content. [K2_K02]
• The student is ready to think and act in an entrepreneurial manner. [K2_K04]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

• Lecture: A written exam assessing students' knowledge through open-ended questions and multiple-choice questions. No materials are allowed during the exam.
• Laboratory Exercises: Assessment based on progress made during each laboratory session.
• Project: Evaluation based on prepared reports and presentations related to a case study covering project initiation, planning, execution, monitoring, and completion.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 51% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university’s electronic systems and during the first class meeting (in each form of classes).

Programme content

The course will cover threats and attacks on cloud infrastructure. The shared responsibility model defining the division of security responsibilities between the cloud provider and the user will be explained. Students will learn about data protection mechanisms, including encryption, cryptographic key management, and access control. Security monitoring through SIEM systems and the integration of DevSecOps into the software development process will be presented. Additionally, compliance with legal regulations and strategies for Disaster Recovery and Business Continuity in the cloud will be discussed.

Course topics

1. Introduction to Cloud Security
• Definition and cloud models (IaaS, PaaS, SaaS)
• Cloud deployment models (public, private, hybrid, multi-cloud)
• Benefits and risks of using cloud services
• Legal regulations and compliance (GDPR, HIPAA, ISO 27001, NIST)
2. Threats and Attacks on Cloud Systems
• Infrastructure layer attacks (DDoS, API attacks, VM exploits)
• Application-layer attacks (injection, XSS, CSRF)
• Data storage and transmission threats (man-in-the-middle, ransomware, data loss)

• Insider threats
3. Shared Responsibility Model in Cloud Security
• Responsibility distribution between cloud providers and users
• Examples of shared responsibility in AWS, Azure, and Google Cloud
• Risk minimization strategies
4. Data Protection Mechanisms in Cloud Computing
• Encryption of data at rest and in transit
• Cryptographic key management (KMS)
• Data masking and tokenization
5. Access Control and Identity Management (IAM)
• IAM roles and policies in AWS, Azure, and GCP
• Multi-Factor Authentication (MFA)
• Least Privilege Access and Zero Trust Security
• Identity federation and Single Sign-On (SSO)
6. Security Monitoring and Threat Detection
• SIEM systems (Security Information and Event Management)
• Cloud monitoring services (AWS CloudTrail, Azure Security Center, Google Security Command Center)
• Anomaly and incident detection
7. Disaster Recovery and Business Continuity in the Cloud
• Data backup and recovery strategies
• Designing resilient cloud systems
• Redundancy and failover strategies
8. Auditing and Compliance in Cloud Security
• Cloud compliance frameworks (CIS, NIST, GDPR, SOC 2)
• Tools for cloud security assessment and auditing
• Case studies: real-world security breaches in cloud environments
Laboratory Exercises and Group Projects
• Hands-on exercises and group projects aligned with lecture topics.

Teaching methods

• Lecture: Multimedia presentation supplemented with examples illustrated on the board and practical demonstrations.
• Laboratory Exercises: Hands-on practical exercises performed individually or in groups using a computer.
• Group Projects: Collaborative project work conducted in teams.

Bibliography

Basic:
Chris Dotson, Bezpieczeństwo w chmurze, Wydawnictwo Naukowe PWN, 2020 Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

Additional:
P. Mishra, E. S. Pilli, R. C. Joshi, “Cloud Security: Attacks, Techniques, Tools, and Challenges”, CRC Press.,
2021 (https://www.amazon.com/Cloud-Security-Attacks-Techniques-Challengesebook/dp/B09MTT5D3T) J. R. Vacca, “Cloud Computing Security: Foundations and Challenges”. CRC Press, 2016 (https://www.amazon.com/Cloud-Computing-Security-Foundations-Challenges/dp/1482260948) C. Dotson, “Practical Cloud Security: A Guide for Secure Design and Deployment”, O'Reilly Media, 2019 (https://www.amazon.com/Practical-Cloud-Security-Secure-Deployment/dp/1492037516)

Breakdown of average student's workload

	Hours	ECTS
Total workload	119	4,00
Classes requiring direct contact with the teacher	64	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	55	2,00