Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Cyber Security in Health

26FS

Studiengang	MSc in Business Information Systems
Stufe	Master
ECTS	3
Modultyp	Wahlpflichtmodul
Modulverantwortliche	Dr. Pascal Moriggl
Anwesenheitspflicht	Attendance is expected
Leitidee / Kurzbeschreibung	This course will examine the critical importance of cybersecurity in health, focusing on the multifaceted challenges and strategies for safeguarding health systems, devices, and data. Students will explore the foundational principles of two primary certification tracks the world offers at the intersection of cyber security and the health industry. Topics covered will blend both management and hands-on skills as essential basics for IT professionals pursuing a career in the health industry with a scoop of cybersecurity. The course aims for students willing to learn both managerial and practical aspects of cybersecurity at an entry-level but with technical or professional experience in a health setting.
Lerninhalt	**1. Management (– GRC)** a. Governance b. Strategy c. Practical: NIST Protect, Detect, Respond, Recover **2. Management (– Information Security)** a. InfSec Program Development b. InfSec Program Management c. +Lab Practice **3. Management (– Incident Management)** a. Incident Readiness b. Incident Operation c. +Lab Practice **4. Medical Environment (– Application Security)** a. Software: Basics, Robustness, Bugs, Secure Usage b. Patch Management c. +Lab Practice **5. Medical Data I (–IAM)** a. Identity and Access Management b. +Lab Practice **6. Medical Data II (– Encryption)** a. Storage b. Encryption c. +Lab Practice **7. Medical Device (–IoT Security)** a. IoT Types b. Issues (OWASP) c. Attack Vectors, Targets d. +Lab Practice

Zu erreichende Kompetenzen

Knowledge and Understanding

- Develop a strong grasp of governance and strategy in information security, particularly in medical informatics.
- Gain expertise in creating, managing, and assessing security programs, emphasizing classification and standards.
- Understand incident readiness, response, and operational management, using tools like Metasploit.
- Learn software security, patch, and vulnerability management for secure medical applications.
- Acquire foundational knowledge in identity and access management (IAM) and encryption to protect medical data.

Application of Knowledge

- Apply governance frameworks and security strategies in medical informatics, following NIST guidelines for protection, detection, response, and recovery.
- Develop security programs that align with organizational goals, including risk management and asset classification.
- Create incident readiness and response plans using practical tools for effective management.
- Implement best practices in software security and patch management to ensure secure medical applications.
- Use IAM and encryption techniques to secure medical data, ensuring compliance with standards.

Judgment

- Critically evaluate the effectiveness of security frameworks, strategies, and programs, making decisions based on risk and organizational needs.
- Assess the comprehensiveness of security programs and the adequacy of controls.
- Judge the effectiveness of application security, patch management, and encryption in safeguarding medical data.

Communication

- Produce clear, concise reports on cybersecurity risks, strategies, and incidents, making them understandable and relevant to managers and non-IT stakeholders.

Voraussetzungen

It is of advantage to have

1. visited at least one course in the area of Machine Learning, Data Science, or Business Intelligence.
2. fundamental programming / CLI / Virtual Machine skills

Lehr- und Lernmethoden

Contact Hours:

- Lecture, Discussion, Group work, Case study

Guided Self-Study:

- Individual work, Working with a partner

Literatur

Required Reading: none

Bemerkungen

none

Modulbewertung

Grade 1-6 (half grades)

Leistungsnachweise

Assignments 100%	
Mündlich / Schriftlich	written
Art der Leistungsbewertung	1-6 (half grades)
Bemerkungen	The practical assignments are introduced during the semester, and must be handed it by the end of the module.

Informationen zur Durchführung

26FS.Cyber Security in Health - Mi - Olten	
Zeit	08:30 - 12:15
Sprache	Englisch
Periodizität	Wöchentlich
Dozierende	Dr. Pascal Moriggl
Nummer	3-26FS.W-M-BIS-E-CSH.EN