Syllabus of Module

8. Information Security and Risks

Lecturer: Ing. Kristina Kopecká

Module Annotation

The aim of the module is to introduce students to cybersecurity and risk management in organizations so that they are able to make managerial decisions in the context of current threats (in particular phishing / BEC, ransomware, exploitation of vulnerabilities, supply chain risks, cloud / SaaS and identity as the new "perimeter"). The module connects technical principles with real business practice, including governance, policies, processes, measurability, and incident management. Emphasis is placed on the regulatory framework relevant to management, especially NIS2 and the new Czech Cybersecurity Act, effective from 1 November 2025.

Module Objective

After completing the course, applicants should be able to:

- understand and use basic information and cybersecurity terminology (asset–threat–vulnerability–impact–risk),
- describe the main current threats (phishing / BEC, malware, ransomware, exploitation of vulnerabilities, third-party / supply-chain attacks) and their typical impacts on an organization,

- explain managerial responsibilities and the practical implications of NIS2 and the Cybersecurity Act for security management in an organization (roles, processes, reporting, auditability),
- propose basic security measures and policies (identity and access management, passwords/MFA, vulnerability management, backups/recovery, secure operation of cloud / SaaS)
- identify key attack vectors and weak points based on a simplified security audit or self-assessment,
- prepare a concise incident management proposal (minimum incident response plan, escalation, communication) and understand its link to regulatory reporting.

Literature

1. HÁK, Igor. *Kapesní příručka pro boj s počítačovou havětí*, Viry.cz; https://www.viry.cz/wp-content/uploads/2018/10/kniha_virycz-2.pdf
2. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
3. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
4. Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí ČSN EN ISO/IEC 27001 a navazující normy řady 27xxx
5. Průvodce novým zákonem o kybernetické bezpečnosti, NÚKIB, 2025, https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti