Syllabus of Module

8. Information Security and Risks

Lecturer: Pavel Matějíček

Module Annotation

The aim of the course is to familiarise students with the issue of cyber security, its basics and their application in the corporate environment. An integral part of this course will be learning about the basic techniques that attackers use to attack organisations, including recommended practices to defend themselves.

Students will learn to recognise phishing, learn about the types of malware and tools used to break into a company's infrastructure, and learn to minimise the risks of compromising the network.

Module Objective

- After completing the course, applicants should be able to:
- understand basic concepts in the field of information security
- know the main principles and concepts associated with social engineering techniques, phishing, targeted APT attacks and malware
- know and be able to use basic techniques of defense against common threats
- set appropriate policies for using passwords, security software, and policies across the organisation's network
- identify the vectors of possible penetration on the basis of a security audit
- effectively cooperate, manage and evaluate the operation of the IT security department in your organisation.

Literature

1. HOOK, 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 and Pavel BAŠTA. CyberSecurity. Prague: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
3. KOLOUCH, Jan. CyberCrime Prague: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.