8. Informační bezpečnost a rizika

Lektor: Pavel Matějíček

Anotace modulu:

Cílem předmětu je seznámit studenty s problematikou kybernetické bezpečnosti, jejími základy a jejich aplikováním ve firemním prostředí. Integrální součástí tohoto kurzu bude seznámení se se základními technikami, které útočníci k napadení organizací využívají včetně doporučených postupů, jak se jim bránit.

Studenti se naučí rozpoznávat phishing, dozví se o druzích malware a nástrojích, které jsou k průnikům do firemní infrastruktury využívány a naučí se minimalizovat rizika kompromitace sítě.

Cíl modulu:

Po absolvování kurzu by uchazeči měli být schopni:

- chápat základní pojmy v oblasti informační bezpečnosti
- znát hlavní principy a pojmy spojené s technikami sociálního inženýrství, phishingu, cílenými APT útoky a malware
- znát a umět používat základní techniky obrany proti běžným hrozbám
- nastavit vhodné zásady používání hesel, bezpečnostního software a politik napříč sítí organizace
- identifikovat vektory možného průniku na základě bezpečnostního auditu

- efektivně spolupracovat, řídit a vyhodnocovat chod oddělení IT bezpečnosti ve své organizaci.

Literatura:

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.