Oddělení CSIRT (Computer Security Incident Response Team)

Vedoucí: Ing. Vladimír Horák

CSIRT (název vznikl použitím prvních písmen z „Computer Security Incident Response Team“) jako operativní tým zaměřený
na reakci na bezpečnostní incidenty počítačové sítě UK. Oddělení úzce spolupracuje s Odborem kybernetické bezpečnosti Rektorátu UK.

Hlavní kompetence a odpovědnost:
- detekce a analýza kybernetických incidentů,
- rychlá reakce na útoky a narušení systémů,
- koordinace obnovy po incidentech,
- incident reporting a vedení dokumentace,
- komunikace s externími CSIRT týmy a orgány činnými v trestním řízení,
- penetrační testování a simulace útoků,
- technická podpora při řešení bezpečnostních problémů,
- monitoring a provoz bezpečnostních nástrojů (SIEM, IDS/IPS),
- analýza malware a forenzní šetření,
- podpora při krizovém řízení v oblasti IT bezpečnosti.

Oddělení CSIRT ve spolupráci s Odborem KB a Výborem KB se podílí na:
- realizaci preventivních opatření s cílem zvyšovat úroveň kybernetické bezpečnosti IT na UK,
- plnění zákonných povinností UK v oblasti kybernetické bezpečnosti,
- řešení bezpečnostních incidentů včetně koordinované reakce na kybernetické útoky, phishing, malware, neautorizovaný přístup apod,
- monitoringu a detekci hrozeb při aktivním sledování univerzitní sítě a systémů včetně identifikace zranitelností a rizikových aktivit