Computer Security Incident Response Team

Leader: Ing. Vladimír Horák

CSIRT (the name came from using the first letters of the Computer Security Incident Response Team) is an operational team focused on responding to security incidents of the CU Computer Network. The department closely cooperates with the Cyber Security Department of the Rector's Office of the CU.

Main competencies and responsibilities:
- detection and analysis of cyber incidents,
- rapid response to attacks and system breaches,
- coordination of recovery after incidents,
- incident reporting and documentation management,
- communication with external CSIRT teams and law enforcement authorities,
- penetration testing and simulation of attacks,
- technical support in solving security problems,
- monitoring and operation of security tools (SIEM, IDS/IPS),
- malware analysis and forensic investigation,
- support in crisis management in the field of IT security.

The CSIRT department in cooperation with the Department of CS and the CS Committee participates in:
- implementation of preventive measures to increase the level of IT cyber security at the CU,
- fulfilment of legal obligations of the CU in the field of cyber security,
- solving security incidents including coordinated response to cyber attacks, phishing, malware, unauthorized access, etc.
- monitoring and detection of threats in active monitoring of university network and systems including identification of vulnerabilities and risky activities