Katolícka univerzita v Ružomberku Hrabovská cesta 1/A, 034 01 Ružomberok				
Metodické usmernenie	**Číslo:** **CZ 00950/2026 RE**	**Zmena: 0** **Počet príloh: 0**	**Dátum vydania:** **14. 04. 2026** **Dátum účinnosti:** **14.04. 2026**	**Počet strán:** **4**

Nahlasovanie a riadenie kybernetických bezpečnostných incidentov

Úvodné ustanovenia

Cieľom tohto metodického usmernenia je ustanoviť jednotný postup pri kybernetickom bezpečnostnom incidente na Katolíckej univerzite v Ružomberku (ďalej len „KU“) tak, aby bol v súlade so:

- zákonom č. 95/2019 Z. z. o informačných technológiách verejnej správy,
- zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
- vyhláškou č. 179/2020 Z. z. o bezpečnostných opatreniach, bezpečnostnej dokumentácii a bezpečnostných incidentoch.

Článok 1
Rozsah pôsobnosti

Metodický postup sa vzťahuje na:

- rektorát, fakulty a všetky ďalšie organizačné súčasti KU,
- zamestnancov.

Článok 2
Kontaktné miesto pre nahlasovanie incidentov

KU určuje centrálne kontaktné miesto pre nahlasovanie kybernetických bezpečnostných incidentov na úrovni rektorátu:

- e-mail: incident.mail@ku.sk,

- telefonicky alebo osobne manažérovi kybernetickej bezpečnosti (MKB).

Kontaktný organizačný útvar: Referát hlavného kontrolóra, riadenia dokumentácie, vnútornej legislatívy a kybernetickej bezpečnosti.

Na úrovni fakúlt sa incidenty nahlasujú prostredníctvom lokálneho IT pracoviska a súčasne na centrálnu adresu incident.mail@ku.sk .

Článok 3
Postup zamestnancov pri kybernetickom incidente

Každý zamestnanec je povinný:

- bezodkladne nahlásiť podozrivú udalosť alebo incident,
- nezasahovať do kompromitovaného systému nad rámec nevyhnutných opatrení,
- zachovať dôkazy a digitálne stopy.

Postup pre zamestnancov rektorátu:

V prípade podozrenia na incident zamestnanec rektorátu:

1. Okamžite vykoná základné opatrenia:
    - odpojí zariadenie od siete (ak je to bezpečné),
    - neotvára podozrivé súbory alebo odkazy.
2. Nahlási incident **e**-mailom na incident.mail@ku.sk, alebo telefonicky na MKB alebo oddeleniu infraštruktúry IT a informačných systémov.
3. Uvedie minimálne tieto informácie:
    - meno a pracovisko,
    - čas zistenia incidentu,
    - opis udalosti,
    - dotknuté zariadenia alebo systémy.
4. Spolupracuje pri riešení a riadi sa pokynmi MKB.

Postup pre zamestnancov fakúlt:

Zamestnanec fakulty postupuje nasledovne:

1. informuje lokálne IT pracovisko fakulty,
2. súčasne nahlási incident na centrálnu adresu incident.mail@ku.sk,
3. dodržiava pokyny MKB a centrálneho IT, lokálneho IT pracoviska fakulty,
4. zabezpečí zachovanie dôkazov (nevypína zariadenie, nemaže súbory, ak to nie je nevyhnutné).

Príklady udalostí, ktoré je potrebné interne hlásiť:

- podozrivé / opakujúce sa e-maily (phishing) vo veľkom rozsahu,
- neoprávnený prístup do systému,

- strata alebo krádež zariadenia,
- únik alebo podozrenie na únik údajov,
- ransomware alebo iný škodlivý kód (malware),
- neobvyklé správanie systému.

Článok 4
Typy incidentu

Typ	Čo sem patrí	Popis
Nežiaduci obsah	Spam Obťažovanie Pornografia Násilie …	Spam – nevyžiadaný hromadný e-mail – znamená, že používateľ nedal povolenie na jeho poslanie a správa je súčasťou väčšieho súboru správ s rovnakým obsahom. Ďalej do tejto skupiny patria e-maily alebo webové stránky s diskriminačným alebo diskreditačným obsahom, s obsahom pornografie, propagácie násilia a podobne.
Škodlivý kód	Vírus Červ Trójsky kôň Spyware Dialler	Softvér, ktorý je zámerne obsiahnutý alebo vložený do systému so škodlivým zámerom. Na aktiváciu kódu je väčšinou potrebná súčinnosť používateľa.
Získavanie informácií	Skenovanie Odpočúvanie Sociálne inžinierstvo	Skenovanie znamená posielanie požiadaviek na systém s cieľom odhalenia jeho slabín. To zahŕňa niektoré testovacie procesy na zistenie informácií o zariadeniach, službách a účtoch, napr. fingerd, DNS požiadavky, ICMP, SMTP (EXPN, RCPT,…) apod. Odpočúvanie zahŕňa sledovanie a zaznamenávanie sieťovej prevádzky za týmto účelom. Sociálne inžinierstvo znamená získavanie informácií od ľudí netechnickým spôsobom (lži, triky, hrozby).
Pokus o prienik	Využitie známej zraniteľnosti Opakované pokusy o prihlásenie	Pokus skompromitovať systém alebo narušiť službu využitím zraniteľnosti so štandardizovaným identifikátorom (napr. CVE), ako napr. pretečenie pamäte, zadné dvierka, XSS (cross side scripting) apod. Patria sem aj opakované neúspešné pokusy o prihlásenie (hádanie, útok hrubou silou), ako aj pokusy o prienik doposiaľ neznámym spôsobom.

	Útok s neznámymi znakmi	
Prienik	Skompromitovanie privilegovaného účtu / obmedzeného účtu /aplikácie Botnet	Úspešné skompromitovanie systému alebo aplikácie (služby). Môže k nemu dôjsť na diaľku využitím známej alebo novej zraniteľnosti, ale aj neautorizovaným lokálnym prístupom.
Nedostupnosť	DoS DDoS Sabotáž	Pri tomto type útokov je systém bombardovaný takým množstvom paketov, že operácie sú oneskorené, alebo systém skolabuje. Príklady vzdialeného útoku typu DoS sú SYN flooding, ping-flooding, E-mail bombing (DDoS: TFN, Trinity,…). Dostupnosť však môže byť obmedzená aj lokálnymi činnosťami (deštrukcia, prerušenie napájania,…).
Ohrozenie bezpečnosti informácií	Neoprávnený prístup k informáciám alebo zmena	Okrem lokálneho zneužitia dát a systémov, bezpečnosť informácií môže byť ohrozená aj úspešným skompromitovaním aplikácie alebo účtu. Patria sem aj útoky, pri ktorých dochádza k zachytávaniu a pristupovaniu k informáciám počas prenosu.
Podvod, sprenevera	Neoprávnené využívanie zdrojov Porušenie autorských práv Prevzatie identity Phishing	Patrí sem využívanie zdrojov na neoprávnené účely vrátane neoprávneného zisku (napr. účasť na ilegálnych reťazových e-mailoch pre dosiahnutie zisku alebo pyramídové schémy). Patrí sem aj predaj a inštalácia nelicencovaných kópií komerčného softvéru alebo iných materiálov chránených autorskými právami. Ďalej sem patria útoky, pri ktorých jedna entita nelegitímne predstiera identitu druhej, aby z toho mala úžitok, ako aj phishing.
Iné		Bezpečnostné incidenty nehodiace sa k žiadnemu typu.

Vypracoval:	**Schválil:**
Ing. Jozef Priesol, PhD., manažér kybernetickej bezpečnosti, kontroly a riadenia dokumentácie	doc. Ing. Jaroslav DEMKO, CSc., rektor