**Sme obeťou kybernetického útoku**

**Návod na postup pri kybernetickom útoku alebo incidente v rezorte školstva**

Tento návod poskytuje inštrukcie pre všetky školské inštitúcie v prípade kybernetického útoku alebo incidentu. V súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a zákonom č. 95/2019 o informačných technológiách vo verejnej správe, je nevyhnutné postupovať podľa nasledujúcich krokov:

**1. Identifikácia kybernetického incidentu**

* **Podozrivé aktivity**: Sledujte a identifikujte nezvyčajné aktivity v systéme, ako sú neautorizované prístupy, neobvyklé spomalenia systému, alebo neočakávané zmeny v konfigurácii.
* **Bezpečnostné upozornenia**: Dbajte na varovné správy z bezpečnostného softvéru (antivírusy, firewally, IDS/IPS systémy).

**2. Ochrana a izolácia**

* **Odpojenie zariadení**: Pokiaľ je to možné, odpojte zasiahnuté zariadenia od počítačovej siete, aby ste zabránili šíreniu škodlivého kódu. Zariadenie nevypínajte pre zachovanie dôkazov. Po vypnutí alebo reštartovaní sa často stratia dôležité dôkazné súbory (napríklad obsah pamäte zariadenia). Vypnite aj adaptér wifi.
* **Upozornenie personálu**: Okamžite informujte všetkých relevantných zamestnancov a vedenie školy o situácii.

**3. Dokumentácia incidentu**

* **Zaznamenanie informácií**: Zaznamenajte všetky relevantné informácie o incidente, ako čas a dátum, typ útoku (<https://www.csirt.gov.sk/typ-incidentu.html>), zasiahnuté zariadenia a akékoľvek pozorované škody.
* **Zachovanie dôkazov**: Uložte všetky digitálne dôkazy, vrátane logov, záznamov o pripojeniach a podozrivých súborov.

**4. Nahlásenie incidentu**

**Kontaktovanie SK-CERT Národného bezpečnostného úradu**

* Email: incident@nbu.gov.sk
* Telefón: +421 2 68 69 2915, +421 903 993 706
* Web: [www.sk-cert.sk](https://www.sk-cert.sk/sk/aktuality/index.html)