KRÍZOVÁ KARTA

# Prvých 60 minút po IT incidente

Krátky postup pre vedenie školy a IT správcu pri ransomware, kompromitovanom účte alebo strate zariadenia. Cieľom prvej hodiny je obmedziť škodu, zachovať dôkazy a zapojiť správnych ľudí.

## 0-10 minút - zastaviť šírenie

- Ak je zariadenie podozrivé, odpojte ho od LAN/Wi-Fi. Nepripájajte k nemu USB médiá.
- Pri aktívnom ransomware izolujte dotknuté segmenty alebo zariadenia. Nezačínajte hromadne mazať ani preinštalovávať.
- Pri kompromitovanom cloudovom účte použite čisté zariadenie na zablokovanie účtu / relácií a reset prístupov.
- Pri strate notebooku alebo telefónu aktivujte vzdialené blokovanie / wipe iba podľa interného postupu a evidujte čas.

## 10-30 minút - zistiť rozsah a zachovať dôkazy

- Zapíšte čas prvého zistenia, kto incident nahlásil a čo presne pozoroval.
- Uložte screenshoty, názvy zariadení, účtov, IP adresy, upozornenia a relevantné logy.
- Zistite, ktoré účty, zariadenia, servery, zdieľania alebo cloudové služby môžu byť dotknuté.
- Neobnovujte produkciu zo záloh, kým nie je jasné, že sa príčina nevráti do obnoveného prostredia.

## 30-60 minút - riadenie, komunikácia, rozhodnutia

- Informujte vedenie školy a určenú zodpovednú osobu / privacy kontakt podľa charakteru incidentu.
- Kontaktujte IT správcu / bezpečnostného partnera a dohodnite jednu osobu, ktorá koordinuje technické kroky.
- Posúďte, či mohlo dôjsť k porušeniu ochrany osobných údajov alebo k incidentu s oznamovacou povinnosťou; lehoty závisia od konkrétneho režimu.
- Pripravte stručnú internú informáciu: čo nefunguje, čo sa nesmie robiť a kedy bude ďalšia aktualizácia.
- Pred obnovou potvrďte čistý bod obnovy, dostupné zálohy a priority kritických služieb.

> Nerobte bez rozmyslu
>
> Neplaťte útočníkovi, nezverejňujte incident na sociálnych sieťach, nemažte logy, nepreinštalujte všetky zariadenia a nepripájajte zálohy do potenciálne kompromitovanej siete bez koordinácie.

Táto karta je prevádzková pomôcka, nie univerzálny incident response plán ani právne stanovisko. Pri vážnom incidente postupujte podľa konkrétneho prostredia a povinností organizácie.