15 NAJČASTEJŠÍCH KYBERNETICKÝCH KATASTROF, KTORÝM SA DÁ PREDÍSŤ:

1. **Nedostatočné fyzické zabezpečenie:** Sieťové prvky, servery a úložiská dát nie sú dostatočne chránené pred neoprávneným prístupom alebo krádežou.

2. **Nezabezpečené sieťové pripojenie:** Prístup do káblovej aj bezdrôtovej siete školy nie je dostatočne chránený, čo umožňuje neoprávnené pripojenie.

3. **Neefektívna štruktúra počítačovej siete:** Sieť nie je logicky rozdelená na časti podľa bezpečnosti (napr. školskí používatelia, infraštruktúra, mobilné zariadenia), čo zvyšuje riziko neoprávneného prístupu k citlivým údajom.

4. **Zanedbanie ochrany pred prírodnými vplyvmi:** IT vybavenie nie je chránené pred poškodením spôsobeným prírodnými živlami (napr. prehrievanie, vlhkosť, prach).

5. **Chýbajúca alebo neaktuálna dokumentácia:** Škola nemá presný prehľad o svojom IT vybavení, sieti a softvérovom zabezpečení, čo sťažuje správu a riešenie problémov.

6. **Nejasné pravidlá pre používanie IT:** Chýbajú jasné smernice pre bezpečné používanie IT v škole alebo s nimi nie sú používatelia pravidelne oboznamovaní.

7. **Slabé heslá a ich správa:** Užívatelia používajú slabé heslá, opakujú ich naprieč účtami alebo ich nechávajú ľahko dostupné.

8. **Slabá ochrana pred internetovými hrozbami:** Nedostatočné zabezpečenie siete kvalitným firewallom pred online nebezpečenstvami.

9. **Chýbajúca alebo nekvalitná antivírusová ochrana:** Škola nemá kvalitnú, centrálne spravovanú ochranu proti malvéru na všetkých zariadeniach.

10. **Nedostatočné vzdelávanie v oblasti bezpečnosti:** Užívatelia (učitelia, žiaci, administratívni pracovníci) nie sú pravidelne školení o bezpečnom správaní online a pri práci s IT.

11. **Nepripravenosť na krízové situácie:** Škola nemá plány na riešenie bezpečnostných incidentov alebo výpadkov systémov, prípadne tieto plány nikdy netestuje.

12. **Nedostatočná odbornosť IT správy:** Osoba zodpovedná za IT nemá potrebné znalosti a kvalifikáciu na efektívnu a bezpečnú správu školskej IT infraštruktúry.

13. **Nadužívanie účtov s vysokými oprávneniami:** Bežní používatelia majú vysoké oprávnenia v systéme, čo zvyšuje riziko závažných bezpečnostných incidentov v prípade zneužitia účtu.

14. **Nedostatočné zálohovanie:** Chýba systematické zálohovanie dát vrátane informácií uložených v cloude, čo môže viesť k strate dôležitých údajov.

15. **Netestovanie obnovy dát:** Škola pravidelne nekontroluje, či je schopná obnoviť zálohované dáta používateľov aj celej IT infraštruktúry.

Viac informácií na webe minedu.sk

DiTEdu Digitálna transformácia vzdelávania a školy
Spolufinancovaný Európskou úniou
PROGRAM SLOVENSKO
MINISTERSTVO ŠKOLSTVA, VÝSKUMU, VÝVOJA A MLÁDEŽE SLOVENSKEJ REPUBLIKY
npi Národní pedagogický institut České republiky