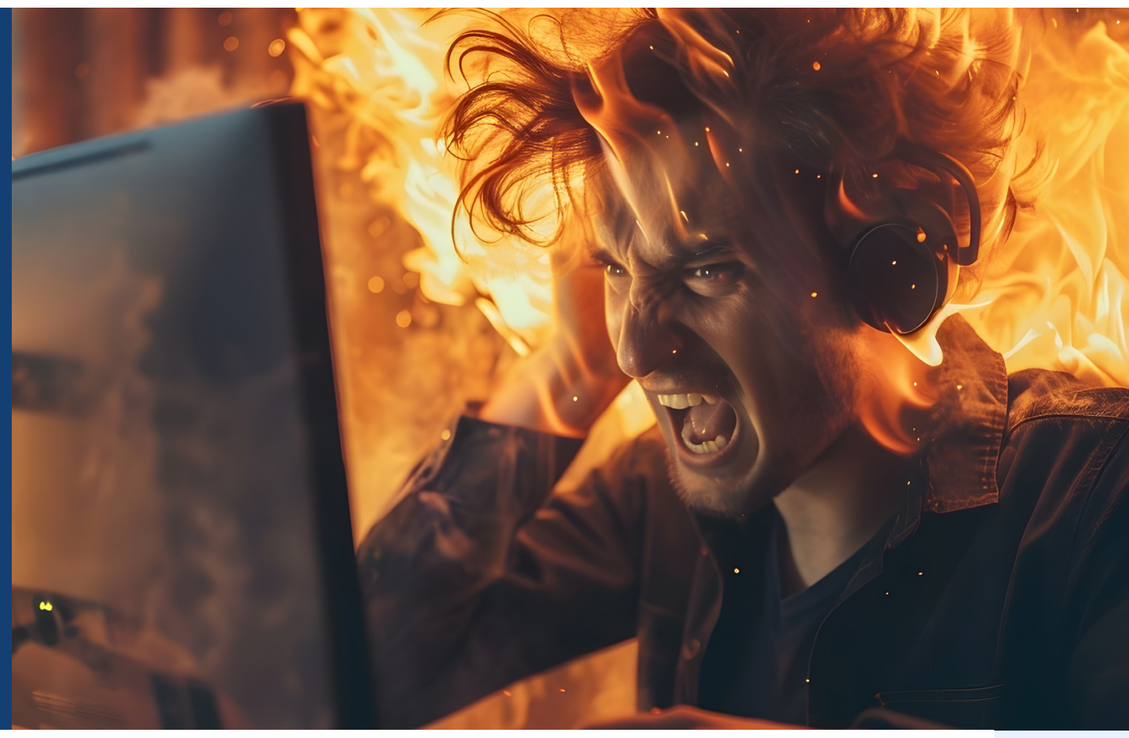
Národní pedagogický institut České republiky

15 NEJČASTĚJŠÍCH KATASTROF, KTERÝM LZE PŘEDEJÍT:



Nedostatečné fyzické zabezpečení: Síťové prvky, servery a úložiště dat nejsou dostatečně chráněny před neoprávněným přístupem nebo krádeží.

Nezabezpečené síťové připojení: Přístup do kabelové i bezdrátové sítě školy není dostatečně chráněn, což umožňuje neoprávněné připojení.

Neefektivní struktura počítačové sítě: Síť není logicky rozdělena na části podle bezpečnosti (např. školní uživatelé, infrastruktura, mobilní telefony), což zvyšuje riziko neoprávněného přístupu k citlivým datům.

Zanedbání ochrany před přírodními vlivy: IT vybavení není chráněno před poškozením způsobeným přírodními živly (např. přehřátí, vlhkost, prach).

Chybějící nebo neaktuální dokumentace: Škola nemá přesný přehled o svém IT vybavení, síti a softwarovém vybavení, což ztěžuje správu a řešení problémů.

Nejasná pravidla pro používání IT: Chybí srozumitelné směrnice pro bezpečné používání IT ve škole nebo s nimi nejsou uživatelé pravidelně seznamováni.

Nepřipravenost na krizové situace: Škola nemá plány pro řešení bezpečnostních incidentů nebo výpadků systémů, případně tyto plány nikdy netestuje.

Slabá ochrana před internetovými hrozbami: Nedostatečné zabezpečení sítě kvalitním firewallem před online nebezpečím.

Chybějící nebo nekvalitní antivirová ochrana: Škola nemá kvalitní, centrálně spravovanou ochranu proti malwaru na všech zařízeních.

Nedostatečné vzdělávání v oblasti bezpečnosti: Uživatelé (učitelé, studenti, administrativní pracovníci) nejsou pravidelně školeni o bezpečném chování online a při práci s IT.

Slabá hesla a jejich správa: Uživatelé používají slabá hesla, opakují je napříč účty nebo je nechávají snadno přístupná.

Nadužívání účtů s vysokými oprávněními: Běžní uživatelé mají vysoká oprávnění v systému, což zvyšuje riziko závažných bezpečnostních incidentů v případě zneužití účtu.

Nedostatečná odbornost IT správy: Osoba zodpovědná za IT nemá potřebné znalosti a kvalifikaci pro efektivní a bezpečnou správu školní IT infrastruktury.

Nedostatečné zálohování: Chybí systematické zálohování dat včetně informací uložených v cloudu, což může vést ke ztrátě důležitých údajů.

Netestování obnovy dat: Škola pravidelně nekontroluje, zda je schopna obnovit zálohovaná data uživatelů i celé IT infrastruktury.

CO DĚLAT, ABY Z TĚCHTO NEDOSTATKŮ NEVZNIKLA PRO VAŠI ŠKOLU KATASTROFA?
VYUŽIJTE BEZPLATNÉHO IT AUDITU A ZJISTĚTE, JAK JE NA TOM VAŠE ŠKOLA.
SJEDNEJTE SI KONZULTACE S IT GURU A SPOLEČNĚ ZLEPŠETE ŠKOLNÍ INFRASTRUKTURU.

Více na digitalizace.rvp.cz

Financováno Evropskou unií NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY