KYBERNETICKÁ BEZPEČNOST PRO OBCE · KNIHOVNIČKA

Reakce na ransomware: prvních 24 hodin krok za krokem

Krizový postup pro IT správce a starostu při útoku ransomware

Konkrétní postup pro prvních 24 hodin po zjištění ransomware útoku. Vychází z metodik NÚKIB.

Načíst na webu

První hodiny rozhodují o tom, kolik dat se zachrání a jak rychle se obec vrátí do provozu. **NEPLAŤTE výkupné** (NÚKIB). Hlášení primárně přes **portal.nukib.gov.cz**; telefonicky +**420 541 110 555** (prac. doba) nebo +**420 725 502 878** (mimo).

- [ ] NUTNÉ 0–15 min: izolovat zasažený systém od sítě — **0–15 min**
  Fyzicky odpojit ethernet kabel, vypnout Wi-Fi. **Nevypínat počítač** — operační paměť obsahuje stopy pro forenzní analýzu.

- [ ] NUTNÉ 15–60 min: vyhodnotit rozsah — co je šifrováno, co ne — **15–60 min**
  Které disky/složky/sdílené adresáře jsou zasaženy? Šíří se to po síti? Zda jsou postiženy zálohy?

- [ ] NUTNÉ 1–24 hod: nahlásit NÚKIB přes Portál NÚKIB — **do 24 hod (§ 15 zák.)**
  Primárně **portal.nukib.gov.cz** (pověřená osoba). V naléhavé situaci telefonicky GovCERT.CZ: +**420 541 110 555** (prac. doba), +**420 725 502 878** (mimo). Náhradní kanál pro nižší režim: abuse@csirt.cz nebo DS h4axdn8.

- [ ] NUTNÉ 1–24 hod: trestní oznámení Policii ČR — **1–24 hod**
  Kybernetické útoky jsou trestné činy. Podejte na kterémkoli oddělení PČR, e-podatelnou, datovou schránkou nebo ústně do protokolu (postup na policie.gov.cz). **Tísňové linky 158/112 NE** — slouží jen pro bezprostřední ohrožení osob nebo majetku.

- [ ] NUTNÉ 2–4 hod: informovat starostu a tajemníka — **2–4 hod**
  Krátký fakt-checked report: rozsah, kdy se to stalo, koho jsme kontaktovali, jaké jsou alternativní cesty.

- [ ] DŮLEŽITÉ 4–8 hod: zajistit forenzní data — **4–8 hod**
  Logy, paměťové dumpy. Zde je zásadní spolupráce s externí firmou (DFIR specialist) — vlastní obec to typicky neumí.

- [ ] DŮLEŽITÉ 8–12 hod: vyhodnotit zálohy a začít obnovu — **8–12 hod**
  Z **off-site** zálohy obnovit jen ověřená čistá data. Vždy na **nové, čisté** infrastruktuře (ne na zasaženém serveru).

- [ ] DŮLEŽITÉ 12–24 hod: komunikovat s občany — **12–24 hod**
  Tisková zpráva, FB, úřední deska. Stručná, věcná, bez paniky. Konkrétní informace o tom, které agendy nejdou a kdy se očekává obnova.

- [ ] DŮLEŽITÉ 24 hod: GDPR — vyhodnotit dopad na osobní údaje — **do 72 hod**
  Pokud únik osobních údajů, **nahlásit ÚOOÚ do 72 hodin** (čl. 33 GDPR). Pokud vysoké riziko, informovat dotčené subjekty.