KYBERNETICKÁ BEZPEČNOST PRO OBCE · KNIHOVNIČKA

Komunikace s občany při incidentu

Co (ne)dělat, když obec čelí kybernetickému útoku

Stručný souhrn pravidel komunikace s veřejností a médii během kybernetického incidentu. Vychází z doložených případů v české veřejné správě.

Načíst na webu

Co dělat ✓

- **První zpráva bez zbytečného odkladu** — věcně, pravdivě.
- **Informujte přes web a sociální sítě** (NÚKIB). Když nejdou, použijte úřední desku, FB, místní noviny, jiný e-mail/telefon.
- Řekněte: co se stalo, koho to ovlivňuje, kdy obnova, kam s dotazy.
- **Pravidelně aktualizujte** — mlčení vzbuzuje paniku.
- **Spolupracujte s NÚKIB** přes portal.nukib.gov.cz; telefon GovCERT.CZ +**420 541 110 555** (prac. doba), +**420 725 502 878** (mimo).

Co nedělat ✗

- **Nezamlčujte útok** — občané to zjistí a důvěra padne víc.
- **Žádné technické detaily** o ransomware (rodina, částka) — pomáhají útočníkům.
- **Neslibujte termín obnovy**, který si nejste jistí.
- **NEPLAŤTE výkupné** (NÚKIB) — postoj „neplatíme" komunikujte jasně.
- **Nedávejte vinu zaměstnancům** — typicky jde o systémové selhání.

Vzor první tiskové zprávy

„Obec [Název] dnes [datum] zjistila kybernetický incident, který omezil dostupnost systémů. Dotčené agendy: [matrika / účetnictví]. **Při pravděpodobném riziku pro práva a svobody osob ohlásíme porušení zabezpečení osobních údajů ÚOOÚ do 72 hod (čl. 33 GDPR); při vysokém riziku informujeme i dotčené osoby.** Spolupracujeme s NÚKIB a Policií ČR. Pro neodkladné záležitosti volejte [tel.]. Aktualizace zveřejníme zde [URL] a na úřední desce. Příklad: Správa služeb hl. m. Prahy (4/2025, Cicada3301) potřebovala týdny na plné obnovení provozu."