KYBERNETICKÁ BEZPEČNOST PRO OBCE · KNIHOVNIČKA

Checklist pro starostu: prvních 90 dní podle z. 264/2025

Klíčové kroky, které by měl udělat každý starosta — i v obci mimo přímou regulaci

Praktický checklist pro starostu, který nastoupil nebo se rozhodl konsolidovat kyber zabezpečení obce. Vychází ze zákona č. 264/2025 Sb. a vyhlášky 410/2025 Sb.

Načíst na webu

Doporučení **NÚKIB pro malé a střední obce**. Cílem není „splnit zákon", ale snížit reálné riziko incidentu. Termíny v jednolistu jsou orientační — zákonné lhůty (ohlášení regulované služby, registrace pověřené osoby) vyplývají z § 13–16 z. 264/2025.

- [ ] NUTNÉ **Určit osobu pověřenou kybernetickou bezpečností** — ihned
  Může to být stávající IT správce s kurzem „Šéfuj kyber" (4–5 h zdarma), nebo **sdílený KB manažer** pro více obcí v rámci ORP — pro malé obce nejefektivnější model (§ 3 vyhl. 410/2025).

- [ ] NUTNÉ **Zjistit, do jakého režimu obec spadá podle z. 264/2025** — do 30 dní
  ORP a Praha 1–22 spadají pod **nižší** povinnosti. Ústřední orgány, kraje, MHMP pod **vyšší**. Ostatní obce mimo přímou regulaci, ale platí pro ně doporučení NÚKIB.

- [ ] NUTNÉ **Vytvořit Přehled bezpečnostních opatření (§ 3 vyhl.)** — do 1 roku od doručení rozhodnutí o registraci
  Inventarizace aktiv: co spravujete (matrika, spisová služba, účetnictví), kde to běží (vlastní server, cloud, dodavatel), kdo má přístup. Bez přehledu nelze chránit.

- [ ] NUTNÉ **Ověřit existenci zálohy off-site a off-line** — do 30 dní
  Záloha na stejném serveru jako data NENÍ záloha. Pravidlo **3-2-1**: 3 kopie, 2 různé typy médií, 1 off-site. Otestujte obnovu (§ 6 vyhl. — řízení kontinuity).

- [ ] DŮLEŽITÉ **Aktualizovat všechny IS a klientské počítače (§ 12 vyhl.)** — do 60 dní
  OS, antivirus, firmware routerů, kancelářský SW. Zastaralé verze jsou nejčastější vstupní bod ransomware.

- [ ] DŮLEŽITÉ **Zapnout MFA u všech administrátorských účtů (§ 8 vyhl.)** — do 60 dní
  Zejména pro e-mail, datovou schránku, účetnictví, VPN. Vyhláška vyžaduje „alespoň dva různé typy faktorů".

- [ ] DŮLEŽITÉ **Připravit postup pro incident a kontakty (§ 15 zák. + GDPR čl. 33)** — do 60 dní
  Prvotní hlášení NÚKIB **do 24 h**, podrobné při významném dopadu **do 72 h**, závěrečná zpráva **do 30 dní**. Paralelně: ÚOOÚ **do 72 h**, pokud mohlo dojít k úniku osobních údajů.

- [ ] DŮLEŽITÉ **Proškolit vedení obce + zaměstnance (§ 4, § 5 vyhl.)** — do 1 roku od doručení rozhodnutí o registraci
  Pro starostu/tajemníka kurz „Vrcholné vedení" (6 h), pro všechny „Dávej kyber". Zdarma na osveta.nukib.gov.cz.

- [ ] DOPORUČENÉ **Plán pro krizovou komunikaci s občany** — do 90 dní
  Při ransomware obec nemůže komunikovat e-mailem ani přes web. Alternativní cesta (fyzická úřední deska, tisková zpráva místním novinám, sociální sítě) musí být připravená.