Nový zákon o kybernetické bezpečnosti – návod pro ředitele krajských úřadů

Tento dokument neslouží jako náhrada platných právních předpisů ani závazný výklad práva. Dokument slouží výhradně jako doplňkový materiál k prezentaci, která proběhla na poradě MV v usedlosti Spiritka dne 19. 11. 2025 v Praze.

Proč se vás to týká

Od 1. 11. 2025 je účinný nový zákon o kybernetické bezpečnosti (nZKB) a související vyhlášky (zejména č. 408/2025 Sb., o regulovaných službách a č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností).

Vyhláška o regulovaných službách řadí „kraj“ mezi poskytovatele regulované služby 1.1 – Výkon svěřených pravomocí v odvětví veřejná správa v režimu vyšších povinností.

„Povinnou osobou“ je kraj jako celek. **Ředitel KÚ** je součástí **vrcholového vedení** a v praxi **nese odpovědnost za to, že kraj zákonné povinnosti plní.**

Krok 1 – Ohlášení regulované služby a komunikace s NÚKIB

Ohlášení regulované služby (§ 6 nZKB)

Ohlášení se podává **přes Portál NÚKIB** a musí být učiněno **do 60 dnů ode dne, kdy kraj splnil podmínky pro registraci** – u krajů se to prakticky kryje s datem účinnosti zákona (1. 11. 2025).

Jako ředitel musíte zajistit, že je určena osoba, která ohlášení zpracuje a podá a že máte interně potvrzeno, jaké údaje o kraji a službě se budou hlásit (název, IČO, popis služeb, kontakty atd.).

Povinná elektronická komunikace

Vyhláška o Portálu NÚKIB (č. 334/2025) stanoví, že **veškerá hlášení (regulované služby, incidenty, další úkony) probíhají primárně přes Portál NÚKIB**.

Ředitel musí zajistit, že úřad má zřízené účty, nastavené procesy, kdo a jak přes Portál komunikuje.

Krok 2 – Governance a role vedení

Vyhláška č. 409/2025 dává vrcholovému vedení (tedy i řediteli KÚ) konkrétní úkoly.

Pro ředitele KÚ z toho plyne, že musí:

1. **Absolvovat prokazatelné školení** pro vrcholné vedení (součást bezpečnosti lidských zdrojů podle § 10 vyhlášky č. 409/2025).
2. **Zajistit stanovení bezpečnostní politiky a cílů ISMS**, kompatibilních se strategickým směřováním kraje.
3. **Integrovat systém řízení bezpečnosti informací (ISMS) do procesů úřadu** (bezpečnost není „jen IT“, ale běžná součást řízení agend, projektů a rozpočtu).
4. **Zajistit zdroje** – personální, finanční i časové – potřebné pro provoz ISMS a plnění povinností.
5. **Interně komunikovat význam kybernetické bezpečnosti**, podporovat kulturu bezpečnosti a „jít příkladem“ (dodržovat vlastní pravidla).
6. **Podílet se na analýze dopadů a řízení kontinuity**, včetně testování plánů kontinuity a obnovy.
7. **Zřídit výbor pro řízení kybernetické bezpečnosti**, určit jeho členy (včetně manažera kybernetické bezpečnosti a alespoň jednoho člena vrcholného vedení) a zajistit jeho pravidelné zasedání a dokumentaci.
8. **Formálně určit bezpečnostní role** (manažer kybernetické bezpečnosti, architekt, garanti aktiv, auditor) a zajistit jejich zastupitelnost a potřebné pravomoci a prostředky.

Krok 3 – Zajištění implementace bezpečnostních opatření

Zákon ukládá poskytovateli regulované služby v režimu vyšších povinností povinnost:

1. **Vymezit stanovený rozsah** (aktiva související s výkonem svěřených pravomocí kraje) – tj. identifikovat primární a podpůrná aktiva, vést jejich evidenci a pravidelně ji aktualizovat (§ 12 nZKB).
2. **Zavádět a provádět bezpečnostní opatření** podle § 14 nZKB a vyhlášky č. 409/2025 (organizační i technická opatření – ISMS, řízení rizik, dodavatelé, řízení přístupu, incidenty, kontinuity, fyzická bezpečnost, sítě, logování atd.).
3. **Pravidelně hodnotit účinnost ISMS** a zpracovávat zprávu o přezkoumání systému; vrcholné vedení se s ní musí prokazatelně seznamovat (§ 3 a § 4 vyhlášky č. 409/2025).

4. **Zajistit audity kybernetické bezpečnosti** v předepsané periodicitě (§ 3 písm. e) vyhlášky č. 409/2025).

V praxi to pro ředitele znamená, že musí:

- *zadat vybudování/rozšíření ISMS pro rozsah výkonu svěřených pravomocí,*
- *schválit a „vlastnit" klíčové dokumenty (politika, koncepce, plán řízení rizik, plán kontinuity),*
- *dohlížet na to, že úřad má nastavené procesy (řízení změn, řízení dodavatelů, přístupy, logování atd.) v souladu s vyhláškou.*

Krok 4 – Incidenty a spolupráce s NÚKIB

Kraj jako poskytovatel v režimu vyšších povinností musí:

1. **Hlásit kybernetické bezpečnostní incidenty NÚKIB** podle § 15–16 nZKB – včetně povinného prvotního hlášení ve stanovené lhůtě a doplňujících informací.
2. **Spolupracovat při zvládání incidentu** – poskytovat informace a součinnost (§ 17 nZKB).
3. **Dodržovat rozhodnutí NÚKIB** (výstrahy, reaktivní protiopatření, opatření za stavu kybernetického nebezpečí).

Ředitel KÚ musí zajistit, aby:

- *existovala **24/7 funkční linka** pro hlášení incidentů,*
- *byly nastaveny vnitřní eskalační postupy (kdo rozhoduje, kdy se hlásí NÚKIB, kdy se informují uživatelé/služby),*
- *úřad byl organizačně připraven plnit rozhodnutí NÚKIB v krizové situaci (včetně pracovních pohotovostí atd., pokud to bude nutné).*

Krok 5 – Dodavatelé a veřejné zakázky

Zákon i vyhláška požadují **řízení bezpečnosti dodavatelů** – identifikaci významných dodavatelů, smluvní požadavky na bezpečnost, řízení rizik dodavatelského řetězce.

Na úrovni kraje to typicky znamená:

- *nastavit **minimální bezpečnostní požadavky do zadávací dokumentace**,*
- *mít přehled o tom, kteří dodavatelé spravují kritické systémy či data,*
- *vyžadovat od nich plnění bezpečnostních opatření (např. logování, šifrování, incident reporting).*

Krok 6 – Kontroly, sankce a osobní odpovědnost

NÚKIB je oprávněn provádět **kontroly plnění povinností**, ukládat **nápravná opatření**, případně i **pozastavit certifikaci** nebo rozhodnout o **zrušení registrace**.

Za nejzávažnější porušení (např. nezavedení opatření, neplnění uložených opatření nebo zákazů dodavatelů) mohou být u subjektů v režimu vyšších povinností uloženy pokuty až **250 mil. Kč nebo 2 % čistého celosvětového ročního obratu**, podle toho, co je vyšší.

Zákon umožňuje i **dočasný zákaz výkonu funkce člena statutárního orgánu** u subjektů v režimu vyšších povinností, pokud svým jednáním zmaří plnění nápravného opatření NÚKIB. Uplatní se jen na funkce, které nejsou „veřejnou funkcí“ ve smyslu § 58 odst. 2 nZKB. **Tedy se tato sankce nevztahuje na post ředitele krajského úřadu.**

Shrnutí pro ředitele krajského úřadu – osobní „to-do list“

Jako ředitel KÚ jsem odpovědný za to, že:

1. **Kraj je řádně registrován jako poskytovatel regulované služby** a údaje v registru jsou aktuální.
2. **Existuje výbor pro řízení kybernetické bezpečnosti**, ve kterém jsem aktivně zapojen.
3. **Máme jmenovaného manažera KB, architekta, garanty aktiv a auditora**, všichni mají mandát a prostředky.
4. **Je definován rozsah a inventář aktiv** pro výkon svěřených pravomocí a pravidelně se aktualizuje.
5. **Probíhá řízení rizik** a existuje plán jejich zvládání navázaný na rozpočet a projekty.
6. **ISMS podle vyhlášky 409/2025 Sb. je zavedený a žije** – školení, procesy, logování, zálohy, testy obnovy, audity.
7. **Máme 24/7 funkční proces pro incidenty**, včetně jasného postupu hlášení NÚKIB.
8. **Řídíme dodavatele** – v zakázkách i smlouvách máme bezpečnostní požadavky a sledujeme jejich plnění.
9. **Jsme připraveni na kontrolu NÚKIB** – víme, kde máme dokumentaci, evidence, zápisy z výboru, výsledky testů a auditů.