NOVÝ ZÁKON O
KYBERNETICKÉ BEZPEČNOSTI

9 **kroků, které neodkládejte!**

§ **Účinnost od 1. listopadu 2025:** zákon č. 264/2025 Sb. rozšiřuje okruh povinných subjektů zhruba na 6 000+ organizací napříč odvětvími. Cílem je, aby kyberbezpečnost řešilo vrcholové vedení firem, ne jen IT oddělení.

1 **ZJISTĚTE, ZDA SPADÁTE DO REGULACE A DO JAKÉHO REŽIMU POVINNOSTÍ**

Proveďte samoidentifikaci a ověřte, zda spadáte do vyššího/nižšího režimu (essential/important). NÚKIB pro tento účel zpřístupnil veřejného průvodce a FAQ. Více info naleznete pod následujícím odkazem - https://portal.nukib.gov.cz/kalkulacka

2 **OHLÁŠENÍ A REGISTRACE U NÚKIB**

Pokud spadáte do regulace, máte 60 dní na ohlášení regulované služby přes Portál NÚKIB (lhůta 60 dnů běží od nabytí účinnosti nového zákona – od 1. 11. 2025).
Po registraci běží obvykle dvě lhůty (od doručení rozhodnutí o registraci):

- 30 dní na doplnění kontaktních údajů,
- 12 měsíců na implementaci bezpečnostních opatření.

3 **NASTAVTE ROLE A ODPOVĚDNOST VEDENÍ**

Určete odpovědnou osobu pro komunikaci s NÚKIB a jasně definujte role a odpovědnost jednotlivých zaměstnanců. Pro vyšší režim je nutné jmenovat manažera kybernetické bezpečnosti. Za dohled nad kyberbezpečností nese osobní odpovědnost vedení firmy.

4 **ANALÝZA RIZIK A ISMS**

Zpracujte katalog aktiv (dat i fyzických prvků infrastruktury), proveďte analýzu rizik a nastavte Information Security Management System (ISMS) v rozsahu vašeho režimu (nižší vs. vyšší). Dokumentujte rozhodnutí a pravidelně revidujte.

5

INCIDENTY: 24 H / 72 H / 1 MĚSÍC

Mějte procesy pro detekci, řešení a hlášení incidentů:

- předběžná zpráva do 24h,
- rozšířené oznámení do 72h,
- závěrečná zpráva zhruba do 1 měsíce.

NATRÉNUJTE TÝM (TABLE-TOP, SIMULACE)

6

BEZPEČNOST DODAVATELŮ

Nastavte požadavky do smluv (minimální standardy, právo na audit, SLA pro reakci na incidenty). U kritických dodavatelů dělejte posouzení rizik a spravujte privilegované přístupy (PAM).

7

INTERNÍ PRAVIDLA, VZDĚLÁVÁNÍ A UDRŽENÍ POVĚDOMÍ

Zaveďte politiky (řízení přístupů, dvoufaktorové ověřování, automatické aktualizace, zálohování/obnova, logování, odpovědnosti), školte zaměstnance a ověřte jejich odolnost vůči kybernetickým hrozbám (phishingové testy).

8

TECHNICKÁ OPATŘENÍ

Prioritizujte MFA, segmentaci sítí, patching, šifrování, monitoring/logování a u vyššího režimu i penetrační testy. Začínejte od kritických systémů.

9

DOKUMENTACE A PŘÍPRAVA NA KONTROLU

Vytvořte jednoduchý registr: co je hotovo, co běží, co se plánuje; přidejte evidence aktiv, rizik, opatření a incidentů. Připravte checklist pro interní sebehodnocení.

Sankce (řádově)

Za závažná porušení až 250 mil. Kč nebo 2 % čistého celosvětového obratu (vyšší z obou). V nižším režimu u vybraných skutků až 175 mil. Kč nebo 1,4 % čistého celosvětového obratu (vyšší z obou). Počítejte i s nápravnými opatřeními a donucovacími pokutami.

Co udělat hned teď:

- Samoidentifikace a potvrzení režimu (důležité: jeden režim na IČO; princip „vyšší bere“).
- Připravit ohlášení do 60 dní od účinnosti/kritérií a počítat s 12 měsíci na implementaci po registraci.
- Vyjasnit role zaměstnanců a odpovědnost vedení.
- Spustit analýzu rizik a ISMS.
- Nastavit incident response (24 / 72 / 1 měsíc).
- Ošetřit dodavatele ve smlouvách a v praxi.
- Začít s MFA, patchingem, logy, segmentací.
- Vést dokumentaci a používat checklist.

Jaký režim platí pro „části firmy“?

Platí pravidlo jeden poskytovatel = jeden režim. Pokud má organizace (jedno IČO) byť jen jednu regulovanou službu ve vyšším režimu, vztáhne se vyšší režim na celou organizaci. Různé režimy v rámci jedné firmy nejsou přípustné — odlišný režim může mít jen jiná právnická osoba (dceřiná společnost, joint venture apod.).

VYUŽIJTE PODPŮRNÉ MATERIÁLY NA PORTÁLU NUKIB: ZDE

- návod k ohlášení regulované služby,
- návod k pověření zástupců organizací,
- návod k hlášení údajů k regulovaným službám,
- materiál k počítání velikosti podniku (včetně vysvětlení výjimek podle § 7 zákona),
- materiál k hlášení kybernetických bezpečnostních incidentů,
- materiál ke stanovení rozsahu řízení kybernetické bezpečnosti,
- materiál k informační povinnosti podle § 19 zákona a
- schéma pro samoidentifikaci v odvětví Výzkum a vývoj.

Netroufáte si sami?

Dejte nám vědět na e-mail gabrielova@komora.cz anebo
sledujte:https://www.komora.cz/sluzby/kalendar-akci/

Zpracovala: Sekce IT a telekomunikací HK ČR k 26.10.2025