



CIO Checklist: Kybernetická bezpečnost dle NIS2

Praktický přehled 44 povinností pro vedení organizace v režimu nižších povinností.

Zákon č. 264/2025 Sb.

Vyhláška č. 410/2025 Sb.

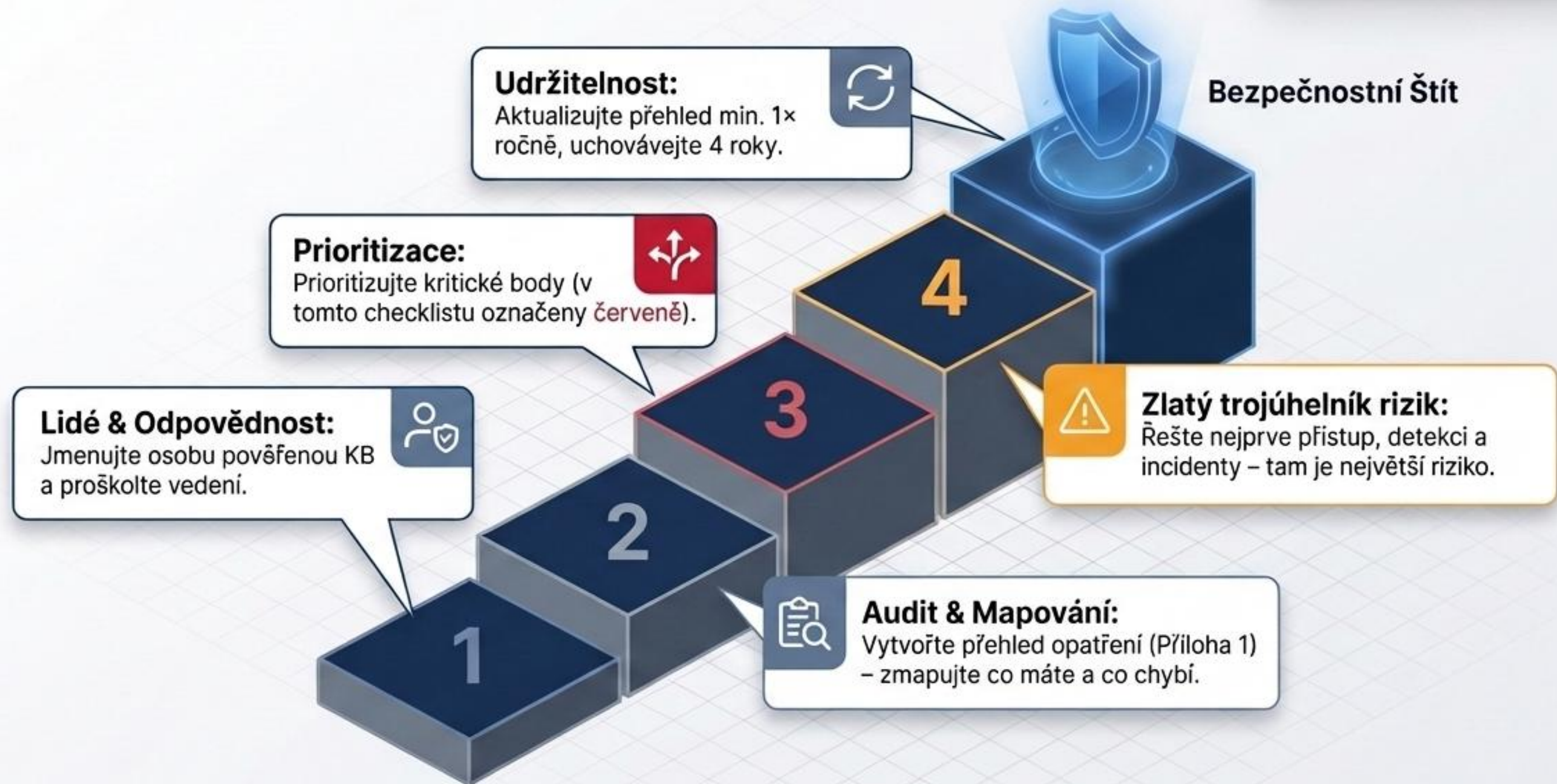
Účinnost: 1. 11. 2025

Zaškrtněte splněné body a sledujte postup implementace napříč 9 bezpečnostními doménami.

Princip – jak začít? Strategie v 5 krocích

Celkový postup: [0/44] · 0%

⚠ Kritické body: [0/13]



Kde začít – První kroky (Fáze 0)

Než se pustíte do technických opatření, zajistěte tyto základy.

Fáze 0: 0/5 splněno

- | | | |
|--------------------------|---|----------|
| ☐ | Určit, zda spadáte do režimu nižších povinností dle zákona 264/2025 Sb. | Kritická |
| ☐ | Jmenovat osobu pověřenou kybernetickou bezpečností (§4a) a zajistit její odborné školení. | Kritická |
| ☐ | Proškolit vrcholné vedení (statutární orgán) v oblasti kybernetické bezpečnosti (§4b). | Kritická |
| ☐ | Vytvořit přehled bezpečnostních opatření dle Přílohy č. 1 – tabulka se stavem všech opatření. | Vysoká |
| ☐ | Stanovit bezpečnostní politiku a dokumentaci ke všem požadovaným opatřením (§3 odst. 3). | Vysoká |





Teplotní mapa rizik: Kde alokovat zdroje

Rozložení 44 povinností napříč bezpečnostními doménami a prioritami.

	Kritická	Vysoká	Střední
Základy (Fáze 0)	3	2	0
 Aktiva a dodavatelé	0	2	1
 Lidé a školení	0	3	2
 Kontinuita (BCDR)	2	2	0
 Identity a přístup	2	3	1
 Detekce událostí	2	2	0
 Řešení incidentů	2	2	0
 Sítě a aplikace	2	3	1
 Kryptografie	0	1	2
 Přezkum a reporting	0	3	1

 Největší koncentrace kritických úkolů leží v doménách Identit, Sítí, Detekce a Řešení incidentů. Zde začněte s implementací.

Řízení aktiv a dodavatelů (§3 odst. 4–6)

0/3

- ☐ Stanovit pravidla pro používání a manipulaci s technickými aktivy. **Vysoká**
- ☐ Při uzavírání smluv zohlednit požadavky Přílohy č. 2 (SLA, audit, exit strategie, incidenty...). **Vysoká**
- ☐ Stanovit bezpečnostní požadavky pro akvizici, vývoj a údržbu aktiv. **Střední**

Bezpečnost lidských zdrojů (§5)

0/5

- ☐ Stanovit politiku bezpečného chování uživatelů dle témat v Příloze č. 3. **Vysoká**
- ☐ Zajistit vstupní a pravidelná školení KB pro všechny zaměstnance. **Vysoká**
- ☐ Zajistit odborná školení pro administrátory a osobu pověřenou KB. **Vysoká**
- ☐ Vést přehledy provedených školení a seznamy školených osob. **Střední**
- ☐ Stanovit pravidla a postupy pro řešení porušení bezpečnostní politiky. **Střední**



🔄 Řízení kontinuity činností (§6)

0/4 📶

Zálohy nejsou vše. Klíčová je schopnost rychlé obnovy dle priorit.

- ☐ Určit odpovědné osoby za kontinuitu činností a obnovu.

Vysoká

- ☐ Stanovit prioritu obnovy primárních aktiv (Pozor: O tomto rozhoduje vrcholné vedení, §4f).

Kritická

Executive Decision

- ☐ Stanovit prioritu technických aktiv, pořadí a postupy jejich obnovy.

Vysoká

- ☐ Vytvářet pravidelné zálohy dat, konfigurací a nastavení pro obnovu po incidentu.

Kritická



Řízení přístupu a identit (§7–8)

0/6 

Checklist

- ☐ Přidělit uživatelům a administrátorům oprávnění na úrovni nezbytně nutné (least privilege). **Kritická**
- ☐ Zavést vícefaktorovou autentizaci (MFA) nebo odolnou kontinuální autentizaci. **Kritická**
- ☐ Oddělit uživatelské a administrátorské účty jedné osoby. **Vysoká**
- ☐ Nastavit přísnou politiku hesel (viz tabulka). **Vysoká**
- ☐ Zajistit pravidelné přezkoumání přístupových práv a odebrání při odchodu. **Vysoká**
- ☐ Zamezit neoprávněnému fyzickému přístupu k aktivům (§7 odst. 2). **Střední**

Požadavky na délku hesla



Uživatel: min. **12** znaků



Administrátor: min. **17** znaků



Technická aktiva: min. **22** znaků



& **SecOps: Od detekce k hlášení NÚKIBu**

Obrana

Detekce a logování událostí (§9) [0/4]

- ☐ Ověřovat data na perimetru sítě, blokovat nežádoucí komunikaci. **Kritická**
- ☐ Nasadit automatickou ochranu před škodlivým kódem (servery + stanice). **Kritická**
- ☐ Zaznamenávat bezpečnostní události (datum/čas, typ, identita, úspěšnost). **Vysoká**
- ☐ Pravidelně a bezodkladně aktualizovat detekční nástroje. **Vysoká**



Reakce

Řešení incidentů (§10) [0/4]

- ☐ Vytvořit metodiku pro posuzování incidentů vč. významnosti dopadu (§14). **Kritická**
- ☐ Zajistit hlášení incidentu s významným dopadem dle §15 zákona. **Kritická**
- ☐ Stanovit únosnou míru újmy pro posouzení významnosti dopadu. **Vysoká**
- ☐ Zajistit vytvoření závěrečné zprávy o vyřešení významného incidentu. **Vysoká**



🌐 Bezpečnost sítě a aplikací (§11–12)

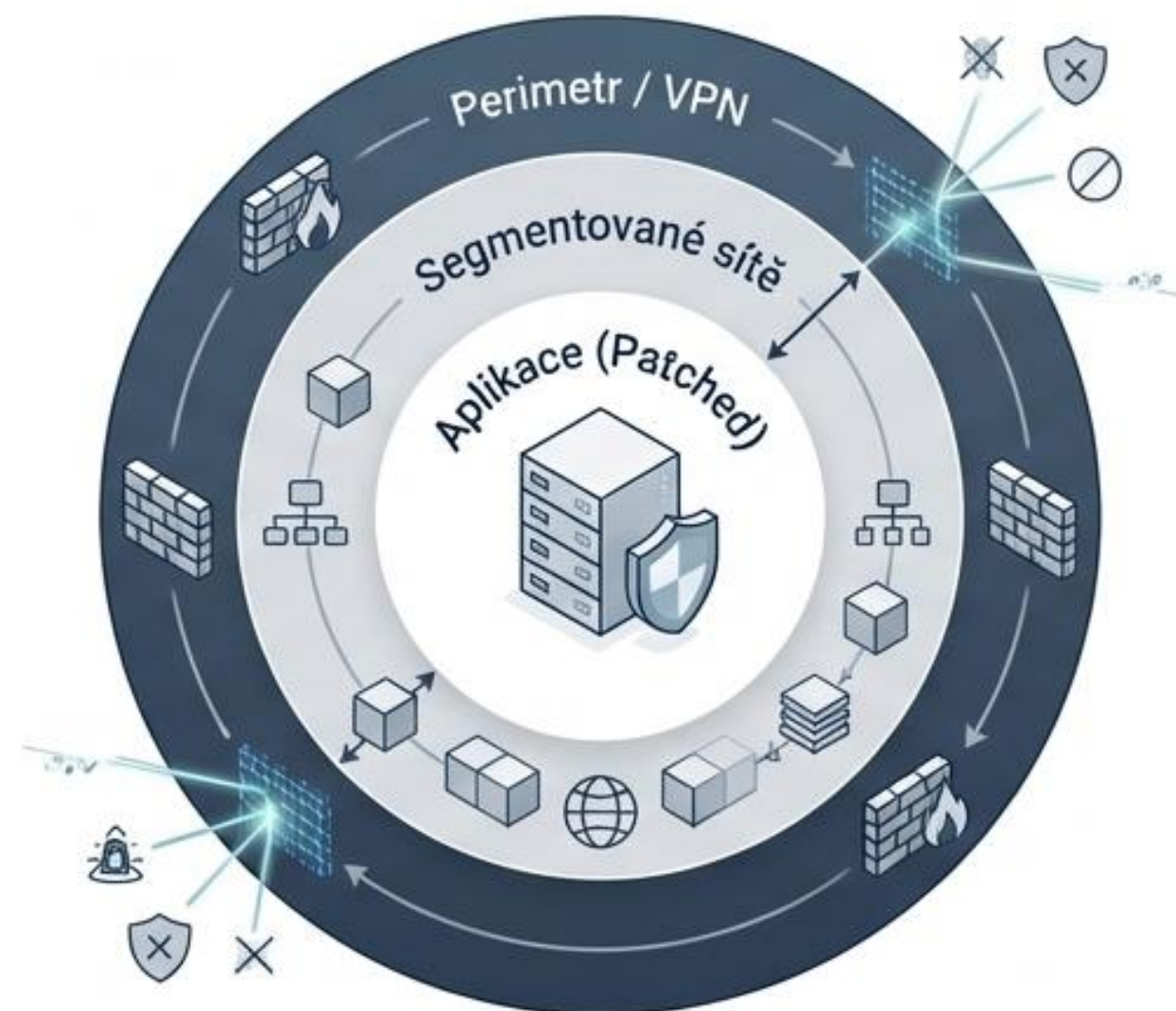


0/6

Ochrana infrastruktury vyžaduje vrstvený přístup (Defense in Depth).

Checklist

- ☐ Segmentovat komunikační síť vč. oddělení provozního a zálohovacího prostředí. **Kritická**
- ☐ Bezodkladně aplikovat schválené bezpečnostní aktualizace (patching). **Kritická**
- ☐ Omezit příchozí a odchozí komunikaci na perimetru na nezbytně nutnou. **Vysoká**
- ☐ Zabezpečit vzdálené připojení (VPN) – důvěrnost, integrita, přehled uživatelů. **Vysoká**
- ☐ Provádět pravidelné skenování zranitelností. **Vysoká**
- ☐ Vést evidenci nepodporovaných technických aktiv a zavést náhradní opatření. **Střední**



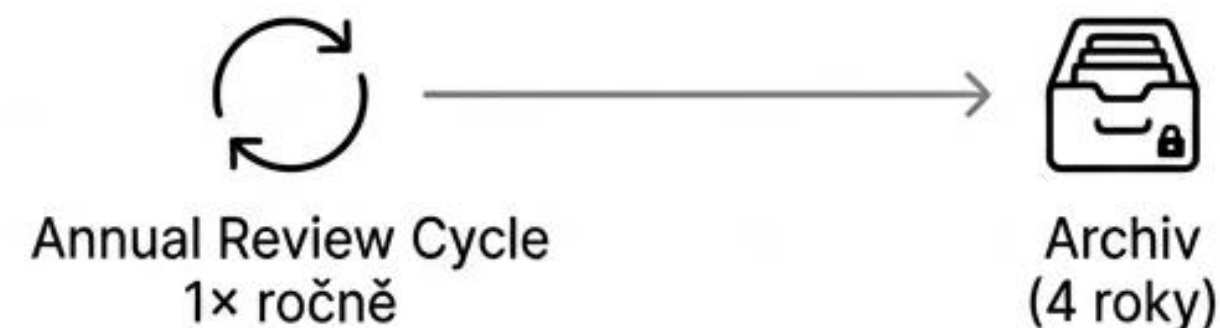


Kryptografie a komunikace (§13) [0/3]

- ☐ Používat aktuálně odolné kryptografické algoritmy dle doporučení NÚKIB.
Vysoká
- ☐ Zajistit bezpečnou hlasovou, audiovizuální, textovou i e-mailovou komunikaci.
Střední
- ☐ Zajistit nouzovou komunikaci v rámci organizace.
Střední

Průběžný přezkum a reporting [0/4]

- ☐ Min. 1× ročně aktualizovat přehled opatření a vyhodnotit účinnost.
Vysoká
- ☐ Pravidelně přezkoumávat a aktualizovat bezpečnostní politiku.
Vysoká
- ☐ Vrcholné vedení se prokazatelně seznamuje se stavem plnění opatření.
Vysoká
- ☐ Uchovávat přehledy opatření a jejich aktualizace min. 4 roky.
Střední





100% shoda vyžaduje čas a kapacitu.

Nemáte interní kapacity na implementaci všech 44 bodů? Pomůžeme vám s vytvořením přehledu opatření, bezpečnostní politiky, školením vedení i zaměstnanců a kompletní implementací požadavků vyhlášky 410/2025 Sb.

obchod@bluepartners.cz
602 177 433