PORTÁL NÚKIB

Dopady nového zákona o kybernetické bezpečnosti na informační systémy veřejné správy

TLP:CLEAR

8. dubna 2026

Verze 1.1

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Dne 1. listopadu 2025 vstoupil v účinnost nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti (nový ZKB). Co to pro mě, jako správce informačního systému veřejné správy, znamená? Jaký význam pro mě mají prováděcí vyhlášky k novému ZKB? A kdo bude kontrolovat, zda své povinnosti řádně plním?

Odpovědi nejen na tyto otázky nabízí následující materiál Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Čtenář se tak níže v tomto textu např. dozví, k jakým změnám dochází v důsledku nabytí účinnosti nového ZKB či jak přistupovat k zavádění bezpečnostních opatření ve vztahu k informačním systémům veřejné správy.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám svůj dotaz napište na regulace@nukib.gov.cz.

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno. Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Změna právní úpravy a její důsledky

Dne 1. listopadu 2025 nabyl účinnosti nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti. V návaznosti na to byl upraven i zákon č. 265/2000 Sb., o informačních systémech veřejné správy (ZoISVS). V důsledku těchto legislativních změn je nutné rozlišovat dvě různé situace, ve kterých se dosavadní správci informačních systémů veřejné správy (ISVS) mohou nově ocitnout. Na některé z nich totiž nový ZKB dopadá, zatímco na jiné nikoli. Co to pro ně znamená, si pojďme dále rozebrat.

2.1 Co když na mě nový ZKB dopadá?

Pokud na dosavadního správce informačního systému veřejné správy nový ZKB dopadá, stává se tzv. **poskytovatelem regulované služby**. V takovém případě bude dle vyhlášky č. 408/2025 Sb., o regulovaných službách, podléhat buď režimu vyšších, nebo nižších povinností. Pokud si nejste jisti, zda do působnosti nového ZKB spadáte, doporučujeme využít naši on-line Kalkulačku na Portálu NÚKIB.

Poskytovatel regulované služby má povinnost zavádět bezpečnostní opatření podle režimu povinností, kterému podléhá. Podrobnosti k zavádění bezpečnostních opatření dle příslušného režimu přitom stanovuje dvojice prováděcích vyhlášek k novému ZKB, a to:

- vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, a
- vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

2.2 Co když na mě nový ZKB nedopadá?

Jestliže správce ISVS do působnosti nového zákona o kybernetické bezpečnosti nespadá, vztahuje se na zabezpečení informačních systémů veřejné správy stále ZoISVS, včetně jeho prováděcí vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy. ZoISVS obsahuje od 1. 11. 2025 nové ustanovení **§ 5b**, které správcům ISVS ukládá povinnost přiměřeného zavádění bezpečnostních opatření na jimi spravované ISVS podle vyhlášky č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

Podle § 5b zákona o informačních systémech veřejné správy platí, že:

*„Správci informačních systémů veřejné správy, kteří **nejsou** poskytovateli regulované služby podle zákona o kybernetické bezpečnosti, jsou povinni na jimi spravované informační systémy veřejné správy zavádět bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností podle § 8, 13 a 14 zákona o kybernetické bezpečnosti, a to **přiměřeně** s ohledem na možné dopady narušení důvěrnosti, integrity a dostupnosti konkrétního informačního systému veřejné správy na činnost jeho správce a jeho schopnost poskytovat své služby občanům, a dále vhodnost a proveditelnost těchto opatření.“*

3 Co znamená zavádět bezpečnostní opatření „přiměřeně“?

Přiměřenost zaváděných bezpečnostních opatření se projevuje ve dvou aspektech.

Prvním z těchto aspektů je **nákladová přiměřenost** zaváděných opatření. To znamená, že náklady na pořízení a zavedení bezpečnostních opatření by neměly převyšovat náklady na řešení dopadu případného kybernetického útoku. Bezpečnostní opatření by tedy měla být zaváděna v míře a na úrovni odpovídající důležitosti zpracovávaných informací a poskytovaných služeb.

Nákladová přiměřenost, zahrnující zohlednění důležitosti určitého ISVS a možných dopadů narušení důvěrnosti, integrity či dostupnosti, se může projevit tím způsobem, že budou zavedena pouze některá bezpečnostní opatření zmíněna ve výše uvedené vyhlášce.

Dále se přiměřenost projevuje tím, že se **správců ISVS týkají pouze požadavky na zavádění bezpečnostních opatření**, a nevztahují se na ně další povinnosti vyplývající z nového ZKB. Nemají tedy mj. povinnost ohlásit poskytování regulované služby, hlásit kontaktní údaje či hlásit kybernetické bezpečnostní incidenty. Z toho důvodu se na ně nevztahuje pasáž vyhlášky, která se týká vyhodnocování významnosti incidentu za účelem posouzení, zda je nutné tento incident nahlásit.

4 Jsou takové změny regulace vůbec potřeba?

V rámci České republiky je vhodné stanovit pravidla kybernetické bezpečnosti jednotně a nevytvářet větší počet různě podrobných standardů. V budoucnu nelze vyloučit rozšíření okruhu poskytovatelů regulovaných služeb dle nového ZKB. Poskytovatelem regulované služby by se tak případně mohli stát i někteří správci ISVS, na které nový ZKB zatím nedopadá.

Požadavek na bezpečnou správu ISVS již nyní stanovuje vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy, jejímž gestorem je Digitální a informační agentura (DIA). Ačkoli v současné době existuje odděleně nový ZKB a ZoISVS, díky výše uvedenému propojení ZoISVS s vyhláškou č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, **nedochází ke vzniku dvojkolejnosti požadavků na kybernetickou bezpečnost**. Naopak dochází ke sjednocování bezpečnostních standardů, a tím i zjednodušení.

5 Kdo bude kontrolovat, zda správci ISVS plní tyto povinnosti?

Pokud se správce ISVS stane poskytovatelem regulované služby dle nového ZKB, provádí kontrolu plnění povinností plynoucích z nového ZKB NÚKIB.

V případě, že na správce ISVS nový ZKB nedopadá, bude kontrola vykonávána dle ZoISVS, a to Digitální a informační agenturou. Nebude tedy docházet ke zdvojování kontrol vykonaných ze strany NÚKIB a DIA.

V rámci kontroly přiměřenosti zavedených bezpečnostních opatření dle vyhlášky o nižším režimu přitom bude Digitální a informační agentura posuzovat, zda zavedená opatření vedou k naplnění povinností dlouhodobého řízení informačních systémů veřejné správy dle ZoISVS a vyhlášky č. 360/2023 Sb. Daný správce je v této souvislosti povinen zejména vést provozní dokumentaci v souladu s § 12 odst. 5 vyhlášky č. 360/2023 Sb. Provozní dokumentace informačního systému veřejné správy, stejně jako informační koncepce, jsou pak dokumenty povinně předkládanými při atestaci dlouhodobého řízení informačních systémů veřejné správy.

6 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
1. prosince 2025	1.0	OREG	Vytvoření dokumentu
8. dubna 2026	1.1	OREG	Oprava drobné chyby (str. 4)