PORTÁL NÚKIB

Stanovení rozsahu řízení kybernetické bezpečnosti

TLP:CLEAR

24. října 2025

Verze 1.0

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Tento dokument popisuje jednotný postup pro stanovení rozsahu řízení kybernetické bezpečnosti (dále jen „KB“) u poskytovatele regulované služby. Právním základem je § 12 zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Stanovení rozsahu řízení kybernetické bezpečnosti je závazné pro poskytovatele regulované služby v režimu vyšších i nižších povinností.

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

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů a popisuje pouze jeden z možných způsobů řešení. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Použité pojmy

- **Aktivum** – je fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováním informací a dat v elektronické podobě.
- **Primární aktiva** – jsou poskytované služby a zpracovávané informace.
- **Podpůrná aktiva** – jsou aktiva, nutná pro zajištění správné funkčnosti, zpracování a uchování primárních aktiv. Podpůrná aktiva jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti aktiv regulované služby. Dále jsou to budovy a jiné ohraničené prostory, ve kterých se tato aktiva nacházejí.
- **Technická aktiva** – jsou technické nebo programové prostředky nebo vybavení. Technická aktiva např. společně tvoří informační systémy nebo průmyslové, řídicí a jiné obdobné specifické systémy.
- **Řízení aktiv** – proces identifikace, evidence, hodnocení a správy aktiv (např. informačních systémů, dat, zařízení, softwaru, osob či služeb), která jsou důležitá pro zajištění kybernetické bezpečnosti organizace.
- **Řízení rizik** – soustavný proces identifikace, hodnocení a zvládání rizik, která mohou mít dopad na bezpečnost informací a kybernetickou bezpečnost systémů.
- **Vlastník/garant aktiv** – osoba zodpovědná za zajištění rozvoje, použití a bezpečnosti konkrétního aktiva (např. informačního systému, zařízení), aby byla zachována jeho důvěrnost, dostupnost a integrita.

3 Zásady a vymezení

- Rozsah řízení KB musí zahrnovat všechna aktiva související s poskytováním regulované služby.
- Od rozsahu řízení KB se odvíjí plnění dalších povinností (zavádění bezpečnostních opatření, hlášení KB incidentů apod.).

4 Stanovení rozsahu řízení KB ve třech krocích

4.1 Krok 1 – Určení všech primárních aktiv v organizaci

Poskytovatel regulované služby nejprve pohlíží na svou organizaci jako na celek. Tedy určí všechna svá primární aktiva v podobě jím zpracovávaných informací nebo poskytovaných služeb. Detail má být takový, aby bylo možné kvalifikovaně rozhodnout, zda aktivum souvisí s regulovanou službou či nikoliv (viz krok 2).

Organizace			
Primární aktivum 1 • služba (interní síťové služby)	Primární aktivum 2 • informace (zákaznická databáze)	Primární aktivum 3 • informace (finanční záznamy)	Primární aktivum 4 • služba (zákaznický helpdesk)

4.2 Krok 2 - Posouzení primárních aktiv

U každého primárního aktiva je nutné posoudit, zda je používáno pro poskytování regulované služby, tedy s ní bezprostředně souvisí. Výsledek (ANO/NE) je nutné řádně evidovat. Tato evidence může být např. součástí evidence primárních aktiv. V případě, kdy primární aktivum nesouvisí s poskytováním regulované služby je možné jej z rozsahu řízení KB vyjmout. Takové vyjmutí je nutné odůvodnit a aktiva vyjmutá z rozsahu řízení KB evidovat.

Aktiva, která nebyla vyjmuta z rozsahu řízení KB, tvoří jeho rozsah.

Souvisí s poskytováním regulované služby	Nesouvisí s poskytováním regulované služby
• PA1 - služba • PA2 - informace	• PA3 - informace • PA4 - služba

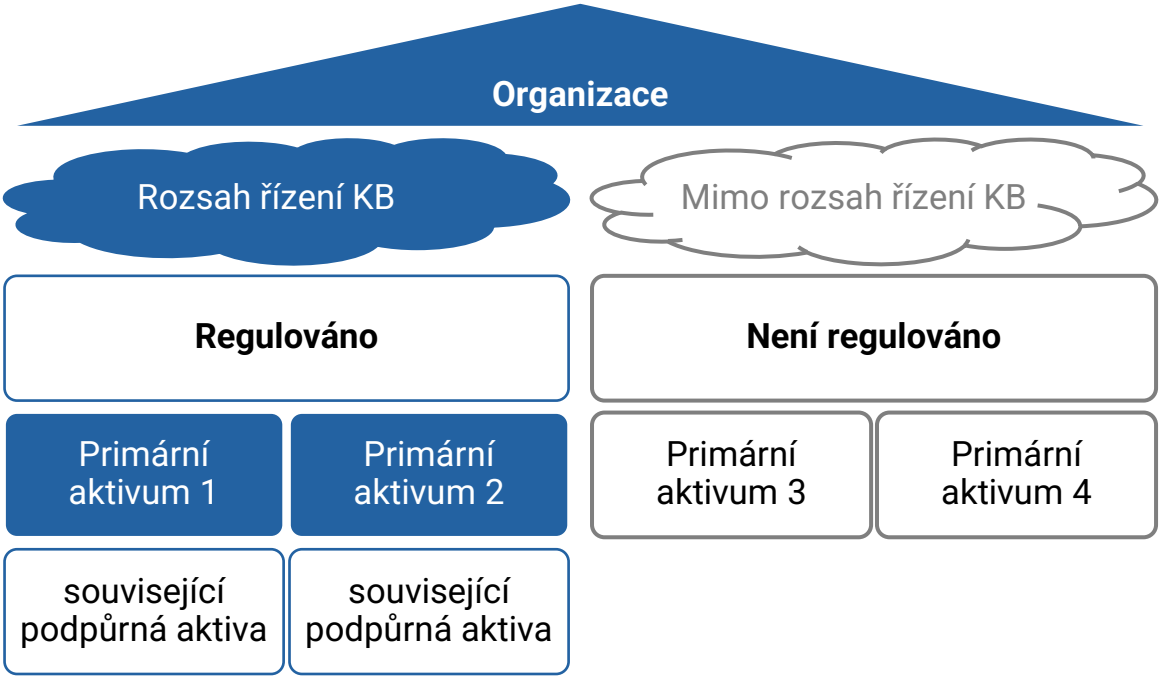
4.3 Krok 3 - Určení podpůrných aktiv

Pro určenou množinu primárních aktiv z rozsahu řízení KB (z kroku 2) se stanoví jejich podpůrná aktiva. Eviduje se vazba na příslušná primární aktiva.

Primární aktivum 1 - služba	Primární aktivum 2 - informace

• zaměstanec
  • odbor právní
• dodavatel
  • dodavatel SW
• technické aktivum
  • SW, HW
• budova
  • serverovna
	• zaměstanec
	  • odbor personální
	• dodavatel
	  • dodavatel SW
	• technické aktivum
	  • koncové stanice
	• budova

Stanovený rozsah řízení KB



5 Evidence a prokazatelnost vymezeného rozsahu

Vymezený rozsah řízení KB se považuje za stanovený v okamžiku, kdy je jeho určení prokazatelně **zdokumentováno**.

To znamená, že je vedena evidence všech primárních aktiv, v níž je **zdůvodněno** případné vyjmutí některých primárních aktiv z rozsahu řízení KB. Totéž platí pro související evidenci podpůrných aktiv.

Evidence zajišťuje jednotnou interpretaci a je klíčová pro případný přezkum. Takto určený rozsah řízení KB je nutné pravidelně přezkoumávat a aktualizovat. Při jeho stanovení je třeba postupovat podle schválené metodiky pro řízení KB.

6 Výchozí rozsah a nová aktiva

Do doby, než je rozsah řízení KB stanoven postupem podle kapitoly 4, platí výchozí rozsah tvořený všemi primárními i podpůrnými aktivy poskytovatele regulované služby.

Nově nabytá nebo změněná aktiva jsou automaticky v rozsahu řízení KB do doby jejich posouzení a určení podle kroků 1–3. V rámci těchto kroků lze rozhodnout o jejich vyjmutí na základě řádného zhodnocení a následně tento postup zdokumentovat v evidenci.

7 Pravidelný přezkum a aktualizace

Poskytovatel regulované služby pravidelně přezkoumává a aktualizuje stanovený rozsah. Interval pro přezkum a aktualizaci není stanoven, nicméně je doporučeno provést ho alespoň jednou ročně a při významných změnách.

8 Následný postup po stanovení rozsahu řízení KB

Po stanovení rozsahu řízení KB poskytovatel regulované služby v režimu vyšších povinností v souladu s vyhláškou č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností dále

- provede řízení aktiv (metodika, klasifikace, vazby, pravidla ochrany),
- provede řízení rizik (metodika, hodnocení rizik, prohlášení o aplikovatelnosti, plán zvládání rizik),
- zavede přiměřená bezpečnostní opatření v míře nezbytné pro zajištění KB regulované služby, v návaznosti na cíle, bezpečnostní potřeby a výsledky hodnocení rizik.

Po stanovení rozsahu řízení KB poskytovatel regulované služby v režimu nižších povinností v souladu s vyhláškou č. 410/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. dále

- provede řízení aktiv (metodika, klasifikace, vazby, pravidla ochrany),
- zavede přiměřená bezpečnostní opatření v míře nezbytné pro zajištění KB regulované služby, v návaznosti na bezpečnostní potřeby.

9 Odpovědnosti

Osoba pověřená KB nebo manažer KB:

- koordinuje postup stanovení rozsahu řízení KB,
- vede a aktualizuje evidenci aktiv,
- předkládá přezkum rozsahu řízení KB vedení.

Vrcholné vedení:

- schvaluje stanovený rozsah řízení KB,
- zajišťuje zdroje a
- dohlíží na pravidelný přezkum.

Vlastníci/garanti aktiv:

- poskytují součinnost při identifikaci a hodnocení aktiv,
- schvalují zařazení/vyjmutí určených aktiv z rozsahu.

10 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**
24. října 2025	1.0	OK	Vytvoření dokumentu