



Stručný metodický postup pro hodnocení aktiv a rizik

TLP:CLEAR

Klikněte nebo klepněte sem a zadejte datum.
Verze 1.0

1 Co se dozvím v tomto dokumentu?

V tomto dokumentu se seznámíte se stručným metodickým postupem pro určování a hodnocení aktiv a rizik v rozsahu řízení kybernetické bezpečnosti. Dokument obsahuje výťah z Průvodce řízením aktiv a rizik dle vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „vyhláška“). Provede Vás přípravou hodnocení, určením a hodnocením primárních i podpůrných aktiv, stanovením jejich vzájemných vazeb a tvorbou relevantních rizikových scénářů založených na hrozbách a zranitelnostech. Dále vysvětluje postup výpočtu a posouzení rizik, možnosti jejich zvládnutí, výběr bezpečnostních opatření a požadavky na související dokumentaci. Dokument je určen jako praktické vodítko, které pomůže nastavit hodnocení aktiv a rizik srozumitelně, jednotně, opakovatelně a tak, aby jeho výsledky byly využitelné pro rozhodování organizace.

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. Právo změny tohoto dokumentu vyhrazeno.

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

2 Základní principy a příprava hodnocení

Použitá metoda je semikvantitativní. Hodnoty se stanovují expertním odhadem podle předem určených stupnic. Účelem není vytvořit maximální počet položek, ale zachytit významná aktiva a relevantní rizika tak, aby výsledky byly srozumitelné, opakovatelné a použitelné pro rozhodování.

2.1 Co musí být připraveno?

Před zahájením musí být znám rozsah řízení kybernetické bezpečnosti a regulovaná služba, k níž se hodnocení vztahuje. Organizace musí mít dokumentovanou metodiku pro určování a hodnocení aktiv a rizik. Metodika stanoví zejména hodnoticí stupnice, pravidla seskupování aktiv, způsob evidence vazeb, vzorec pro výpočet rizika, kritéria akceptovatelnosti a způsob schvalování výsledků.

Současně je nutné shromáždit podklady o službách, procesech, informačních systémech, infrastruktuře, uživateli, dodavatelích, právních a smluvních povinnostech, kybernetických bezpečnostních incidentech, auditech kybernetické bezpečnosti, skenování zranitelností, penetračních testech a významných změnách.

2.2 Doporučený postup přípravy

Krok 1: Vymezte předmět hodnocení

Určete regulovanou službu, organizační a technický rozsah, rozhraní vůči externím systémům a případné logické části.

Krok 2: Shromážděte podklady

Získejte procesní a architektonickou dokumentaci, seznam služeb a informačních systémů, smlouvy, legislativní požadavky, evidence majetku a výsledky kontrolních a bezpečnostních činností.

Krok 3: Nastavte jednotná pravidla

Schvalte stupnice, výpočet, akceptační meze, způsob evidence odůvodnění a pravidla pro řešení nejasných nebo hraničních případů.

Krok 4: Naplánujte rozhovory

Připravte hodnoticí jednání s garanty aktiv, vlastníky procesů, IT, správci smluv a dalšími relevantními odbornými pracovníky.

3 Primární aktiva

Primárními aktivy jsou poskytované služby a zpracovávané informace v rozsahu řízení kybernetické bezpečnosti. Jejich určování začíná u účelu organizace a regulované služby.

3.1 Určení primárních aktiv

Nejprve sepište činnosti, které vytvářejí hodnotu nebo zajišťují regulovanou službu. U každé služby popište její účel, uživatele, hlavní vstupy a výstupy a související zákonné nebo smluvní požadavky. Následně určete informace, bez nichž službu nelze poskytovat.

Služby a informace vzájemně propojte. Jedna služba zpravidla pracuje s více informačními aktivy a stejné informace mohou podporovat více služeb. U každého aktiva ověřte, zda spadá do rozsahu řízení kybernetické bezpečnosti. Případné vyloučení musí být zdůvodněno a nesmí vést k opomenutí aktiva, které ovlivňuje kybernetickou bezpečnost regulované služby.

Seskupování do typových aktiv

Do jednoho typového aktiva slučujte pouze prvky s obdobnou povahou, významem a působením stejných hrozeb a zranitelností. Příliš široká skupina aktiv může vést k zavádění plošných bezpečnostních opatření, která ne vždy odpovídají skutečným potřebám. Příliš jemné členění vytváří neřiditelné množství položek.

3.2 Hodnocení primárních aktiv

Primární aktiva se hodnotí minimálně z pohledu důvěrnosti, integrity a dostupnosti. Organizace může samostatně posuzovat také ztrátu dat, čímž získá vstupy pro řízení kontinuity činností a nastavení zálohování. Hodnotí se dopad narušení aktiva, nikoli pravděpodobnost vzniku události.

Při hodnocení uvažujte realistický nejhorší možný scénář a nezohledňujte již zavedená bezpečnostní opatření. Posuzujte přímé následky narušení. Příčiny, pravděpodobnost a účinnost opatření patří až do hodnocení rizik. Napříč organizací musí být používána stejná stupnice a stejný způsob výkladu. Každou výslednou hodnotu písemně odůvodněte. Služba zpravidla přebírá nejvyšší hodnoty jednotlivých atributů z navázaných informačních aktiv.

U **důvěrnosti** se ptejte, komu a v jakém rozsahu by se informace mohly neoprávněně zpřístupnit. U **integrity** posuzujte následky neoprávněné nebo náhodné změny a rozdíl mezi malou a rozsáhlou modifikací. U **dostupnosti** stanovte, od jaké délky výpadku začínají vznikat jednotlivé úrovně dopadu. U **ztráty** obdobně určete, jak stará data lze ještě obnovit bez významných následků a jaké dopady by měla úplná ztráta.

Hodnotící stupnice jsou uvedeny v příloze č. 1 vyhlášky.

3.2.1 Oblasti, které je nutné posoudit

U každého relevantního atributu posuďte dopady na osobní údaje, právní a smluvní povinnosti, vnitřní řízení a kontrolu, veřejné a ekonomické zájmy, poskytování důležitých služeb, běžné činnosti, pověst

organizace, bezpečnost a zdraví osob, mezinárodní vztahy a uživatele regulované služby. Oblasti lze metodicky sloučit.

3.3 Praktické vedení rozhovoru

Krok 1: Vysvětlete způsob hodnocení

Garant musí rozumět tomu, že se posuzuje úplné narušení konkrétního atributu a že stávající opatření se v této fázi neuvažují.

Krok 2: Vyberte relevantní oblasti

Společně určete, které oblasti dopadu se aktiva skutečně týkají a které jsou nerelevantní.

Krok 3: Projděte každý atribut

Samostatně projděte důvěrnost, integritu, dostupnost a případně ztrátu. U dostupnosti a ztráty používejte předem schválené časové řezy.

Krok 4: Zaznamenejte odůvodnění

Nestačí uvést číslo. Popište konkrétní následek, časový okamžik jeho vzniku a důvod zvolené úrovně.

Krok 5: Proveďte kalibraci

Porovnejte hodnocení s obdobnými aktivy a odstraňte nelogické rozdíly, nadhodnocení nebo podhodnocení.

Krok 6: Potvrďte výsledek

Výsledek nechte potvrdit garantem nebo gestorem a zaznamenejte datum.

4 Podpůrná aktiva a jejich vazby

Podpůrná aktiva umožňují fungování primárních aktiv. Patří sem technické vybavení, komunikační a programové prostředky, budovy a jiné ohraničené prostory, lidské zdroje, dodavatelé a externí systémy či služby.

4.1 Jak podpůrná aktiva určit

Pro každé primární aktivum zjistěte, kde je vytvářeno, zpracováváno, přenášeno, ukládáno a zálohováno. Určete servery, databáze, aplikace, síťové prvky, pracovní stanice, bezpečnostní technologie, lokality a podpůrné služby. Současně určete uživatele, administrátory, správce, vývojáře, dodavatele a osoby odpovědné za smluvní vztahy.

Granularitu zvolte tak, aby bylo možné určit konkrétní hrozby, zranitelnosti a bezpečnostní opatření. Pokud je aktivum vymezeno příliš obecně, opatření se zavádějí plošně i tam, kde nejsou potřebná. Při příliš podrobném členění vzniká množství položek, které organizace nedokáže průběžně spravovat. U každého podpůrného aktiva proto musí být zřejmé, co přesně zahrnuje a která primární aktiva podporuje.

4.2 Hodnocení podpůrných aktiv a jejich vazby

Hodnocení podpůrného aktiva musí být konzistentní s hodnotami primárních aktiv. Organizace může zvolit přímé dědění hodnot, individuální posouzení nebo výpočet založený na síle vazby. **Přímé dědění** je rychlé, ale může vést k nadhodnocení. **Individuální posouzení** je přesnější, avšak kapacitně náročné. **Výpočet přes váhu vlivu** lze automatizovat, ale musí být dobře kalibrován a následně odborně přezkoumán.

5 Hrozby, zranitelnosti a rizikové scénáře

Zranitelnost je slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito hrozbou. Katalog zranitelností vychází z přílohy č. 3 vyhlášky a může být rozšířen o zranitelnosti specifické pro prostředí organizace.

Hrozba je okolnost, událost nebo jednání, které může aktivum poškodit. Katalog hrozeb musí pokrýt úmyslné, neúmyslné i přírodní nebo provozní zdroje a vychází z přílohy č. 3 vyhlášky.

5.1 Vytvoření scénářů

Nevytvářejte kombinace všeho se vším. Pro každé aktivum vyberte pouze zranitelnosti, které se u něj mohou skutečně vyskytovat, a hrozby, které mohou danou zranitelnost využít. Scénář musí určit aktivum, zranitelnost, hrozbu, dotčený atribut a srozumitelný popis následku.

Příklad rizikového scénáře

Databázový server agendového systému používá zastaralý operační systém a aktualizace se zavádějí nepravidelně. Znamá zranitelnost může být zneužita škodlivým kódem, což může vést k nedostupnosti databáze a narušení integrity záznamů.

6 Hodnocení rizik

Hodnocení rizik zahrnuje analýzu relevantních kombinací, určení rizik a porovnání výsledku s kritérii akceptovatelnosti. Pro každé riziko musí být dohledatelné vstupní hodnoty, odůvodnění a rozhodnutí o dalším nakládání.

Riziko = dopad, tedy hodnota příslušného atributu aktiva × hrozba × zranitelnost

6.1 Výpočet a rozhodnutí

Krok 1: Vyberte relevantní atribut

Použijte hodnotu atributu, který může daná hrozba narušit. Pokud scénář zasahuje více atributů, postupujte podle pravidel vlastní metodiky.

Krok 2: Stanovte hodnotu hrozby

Vycházejte ze zkušeností, statistik, kybernetických bezpečnostních incidentů, varování, informací o hrozbách a konkrétních podmínek aktiva.

Krok 3: Stanovte hodnotu zranitelnosti

Posuďte skutečný stav a účinnost bezpečnostních opatření. Pouhá existence dokumentu nebo technologie neprokazuje účinnou ochranu.

Krok 4: Vypočítejte riziko

Použijte schválený vzorec.

Krok 5: Porovnejte výsledek s kritérii akceptovatelnosti

Zařaďte riziko do schválené úrovně a rozhodněte, zda je akceptovatelné.

Krok 6: Zaznamenejte další postup

Uveďte způsob zvládnutí, odpovědnost, navržené opatření, termín a předpokládané zbytkové riziko.

7 Zvládání rizik a dokumentace

7.1 Volba způsobu zvládání

Akceptace se použije pouze v mezích stanovených metodikou; akceptované riziko se nadále eviduje a monitoruje. **Redukce** spočívá v zavedení organizačních nebo technických opatření, která zpravidla snižují zranitelnost. **Eliminace** mění řešení tak, aby riziková situace přestala existovat. **Vyhnutí** znamená omezení nebo ukončení rizikového aktiva či činnosti. **Přenesení nebo sdílení** zapojuje třetí stranu, avšak organizace si zachovává odpovědnost za to, že riziko bude adekvátně řešeno.

7.2 Výběr bezpečnostních opatření

Bezpečnostní opatření musí přímo reagovat na zjištěnou zranitelnost a hrozbu. Při výběru zohledněte legislativní požadavky, technickou účinnost, náklady, dostupné lidské a finanční zdroje a dopady do provozu. Pokud cílové opatření nelze zavést okamžitě, stanovte dočasná kompenzační opatření. Po zavedení vždy ověřte účinnost a přepočítejte zbytkové riziko. Výjimky používejte pouze ojediněle, časově je omezte, zdůvodněte a pravidelně přezkoumávejte.

7.3 Plán zvládání rizik

Plán zvládání rizik propojuje jednotlivá rizika s konkrétními bezpečnostními opatřeními. U každého bezpečnostního opatření musí popis, cíle a přínosy, určení osoby zajišťující zavedení, předpokládané lidské, finanční a technické zdroje, termín zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a konkrétní způsob realizace. Plán zvládání rizik se průběžně aktualizuje podle stavu realizace bezpečnostních opatření.

7.4 Zpráva o hodnocení rizik

Zpráva o hodnocení rizik shrnuje rozsah a použitou metodu hodnocení, hlavní výsledky, přehled akceptovatelných a neakceptovatelných rizik a navržená bezpečnostní opatření. Informace musí být zpracovány tak, aby výbor pro řízení kybernetické bezpečnosti nebo vrcholné vedení mohly na jejich základě přijmout odpovídající rozhodnutí.

7.5 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti obsahuje všechna požadovaná bezpečnostní opatření, jejich stav a způsob zavedení a u nezavedených opatření také odůvodnění a případná náhradní opatření.

8 Přezkoumání hodnocení rizik

Řízení aktiv a rizik je kontinuální proces. Hodnocení rizik se aktualizuje pravidelně jednou ročně a při významných změnách.

Přezkoumání hodnocení rizik proveďte také při změně rozsahu řízení kybernetické bezpečnosti nebo regulované služby, vzniku nové služby, významné změně informačního systému, sítě, technologie nebo architektury, při nové hrozbě či zranitelnosti, po vydání varování nebo protiopatření, po kybernetickém bezpečnostním incidentu, auditu nebo kontrole v oblasti kybernetické bezpečnosti, skenování zranitelností nebo penetračním testu a při změně významného dodavatele, smluvního vztahu nebo umístění aktiva.

8.1 Kontrolní seznam dokončení hodnocení rizik

- Rozsah řízení kybernetické bezpečnosti je jednoznačně stanoven.
- Metodika je schválena, srozumitelná, jednoznačná a umožňuje opakování hodnocení za srovnatelných podmínek.
- Jsou určena všechna primární aktiva včetně jejich garantů, vazeb, hodnot a odůvodnění.
- Podpůrná aktiva odpovídají skutečné architektuře a jsou přiměřeně detailní.
- Vazby mezi podpůrnými a primárními aktivy jsou řádně zaznamenány.
- Katalogy hrozeb a zranitelností jsou přizpůsobeny podmínkám a specifikům prostředí organizace.
- Hodnocení rizik zahrnuje všechny relevantní kombinace aktiv, hrozeb a zranitelností.
- Rizika jsou porovnávána se schválenými kritérii akceptovatelnosti a u každého z nich je rozhodnuto o jeho akceptaci, nebo neakceptaci.
- Pro každé neakceptovatelné riziko je stanoveno konkrétní bezpečnostní opatření, odpovědná osoba, termín realizace a potřebné zdroje.
- Je zpracována zpráva o hodnocení rizik, plán zvládání rizik a prohlášení o aplikovatelnosti.
- Jsou stanoveny pravidelné termíny přezkoumání hodnocení rizik.

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 sdílena 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
2. října 2026	1.0	Odbor kontroly	Vytvoření dokumentu