**Smernica výkonu analýzy rizík a analýzy dopadov**



# Obsah

[Obsah 2](#_Toc136531172)

[1 Správa dokumentu 3](#_Toc136531173)

[2 Účel 4](#_Toc136531174)

[2.1 Právny základ a normatívne odkazy 4](#_Toc136531175)

[3 Výkon analýzy rizík – kvalitatívna analýza rizík 5](#_Toc136531176)

[3.1 Stanovenie kontextu rizika 5](#_Toc136531177)

[3.1.1 Identifikácia aktív a ich vlastníkov 5](#_Toc136531178)

[3.1.2 Identifikácia hrozieb 5](#_Toc136531179)

[3.1.3 Identifikácia zraniteľností 5](#_Toc136531180)

[3.1.4 Odhad dopadov 6](#_Toc136531181)

[3.1.5 Identifikácia existujúcich opatrení 6](#_Toc136531182)

[3.1.6 Závažnosť rizík 6](#_Toc136531183)

[3.2 Fázy kvalitatívnej analýzy rizík 6](#_Toc136531184)

[3.3 Identifikácia scenárov rizík 7](#_Toc136531185)

[3.4 Posúdenie rizika kvalitatívnou metódou 7](#_Toc136531186)

[3.5 Závažnosť rizika 10](#_Toc136531187)

[3.6 Návrh bezpečnostných opatrení 10](#_Toc136531188)

[4 Výkon analýzy dopadov (BIA) 11](#_Toc136531189)

[4.1 Fázy výkonu analýzy dopadov na činnosti organizácie 11](#_Toc136531190)

[4.2 Zber vstupných dát 11](#_Toc136531191)

[4.3 Výstupy z analýzy dopadov 12](#_Toc136531192)

[4.3.1 Stanovenie hodnôt RTO a RPO 12](#_Toc136531193)

# Správa dokumentu

Dokument „Smernica výkonu analýzy rizík a analýzy dopadov“ je vzorovým dokumentom slúžiacim pre potreby orgánov verejnej moci. Vytvorený vzor dokumentu nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument má aj svoj metodický rozmer, takže je ho možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorené dokument nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj „MIRRI“) nezodpovedá za nesprávne použitie predmetného dokumentu zo strany organizácie. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétnej organizácie. Dokument je potrebné upraviť na základe reálnych potrieb a špecifického prostredia organizácie.

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov. Dokument je výstupom pilotného projektu na ktorý nadväzuje Reforma Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

Súčasťou každého dokumentu adaptovaného do prostredia organizácie je aj nasledovný zmenový list obsahujúci informácie minimálne v nasledovnom rozsahu:

|  |  |
| --- | --- |
| **Verzia** |  |
| **Garant dokumentu** |  |
| **Dátum poslednej revízie** |  |
| **Dátum vydania** |  |
| **Dátum účinnosti** |  |

# Účel

Účelom tohto dokumentu je popísať postup výkonu analýzy rizík a analýzy dopadov v organizácii.

Nakoľko je podrobný postupy výkonu analýzy rizík a analýzy dopadov bližšie popísaný v rámci dokumentu „Metodika analýzy rizík a analýzy dopadov“, cieľom tohto dokumentu je organizáciám priblížiť konkrétne kroky týkajúce sa výkonu oboch analýz.

Táto smernica spĺňa požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti resp. zákona č. 95/2019 Z. z. informačných technológiách vo verejnej správe.

## Právny základ a normatívne odkazy

Táto smernica sa opiera najmä o nasledovné právne predpisy a technické normy:

* Metodika analýzy rizík kybernetickej bezpečnosti vypracovaná Národným bezpečnostným úradom,
* Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti,
* Vyhláška NBÚ č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
* Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
* ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy),
* ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy)
* ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy),

# Výkon analýzy rizík – kvalitatívna analýza rizík

Táto kapitola v krátkosti popisuje postup výkonu kvalitatívnej analýzy rizík. Tento spôsob výkonu analýzy rizík používa na definovanie rizikových faktorov slovné hodnoty, ktoré sú pre väčšinu používateľov zrozumiteľnejšie a prijateľnejšie.

## Stanovenie kontextu rizika

Pred začiatkom výkonu analýzy rizík je potrebné si bližšie zadefinovať kontext, ktorom organizácia analýzu rizík vykonáva. Na tento účel je potrebné zaoberať sa najmenej nasledujúcimi činnosťami:

* identifikácia aktív a ich vlastníkov,
* identifikácia zraniteľností,
* identifikácia potenciálnych hrozieb,
* odhad dopadov,
* odhad pravdepodobností,
* identifikácia existujúcich opatrení.

### Identifikácia aktív a ich vlastníkov

V rámci prípravy na výkon analýzy rizík si organizácia vytvára prehľadný zoznam informačných aktív a ich vlastníkov. Vytvorenie daného zoznamu je kľúčové, pretože takýto zoznam je jedným z hlavných vstupov do analýzy rizík a tiež smeruje k tomu, aby nedošlo k opomenutiu žiadneho kľúčového informačného aktíva v rámci procesu určovania závažnosti rizika.

### Identifikácia hrozieb

Hrozba má vo všeobecnosti potenciál poškodenia aktív, môže byť úmyselná, alebo náhodná, príp. spôsobená vplyvom prostredia pre udalosti, ktoré vznikajú nezávisle od ľudskej činnosti.

V rámci výkonu analýzy rizík pracuje organizácia s katalógom hrozieb, ktorý napomáha lepšej identifikácii všetkých relevantých hrozieb.

Národný bezpečnostný úrad (NBÚ) v rámci svojej činnosti pripravil Katalóg hrozieb obsahujúci viac ako 100 rôznych hrozieb v 15 kategóriách. Organizácia môže tento katalóg vytvorený zo strany NBÚ využiť pri príprave vlastného relevantného katalógu hrozieb.

Ďalšími zdrojmi pre katalóg hrozieb sú informácie o hrozbách získané v rámci poučenia z incidentov, informácie od vlastníkov aktív, od používateľov a informácie z ďalších zdrojov vrátane externých katalógov hrozieb.

### Identifikácia zraniteľností

Zraniteľnosť je takým miestom v prostredí IS resp. organizácie, ktoré má potenciál byť zneužité hrozbou a spôsobiť negatívny dopad na informačné aktíva organizácie, alebo organizáciu ako celok.

Identifikáciu uvažovaných zraniteľností organizácia udržiava v rámci Katalógu zraniteľností.

### Odhad dopadov

Identifikované typy dopadov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti sú uvedené v zozname typov dopadov.

Popis dopadov v rámci scenárov rizík je realizovaný uvedením typu alebo identifikátora typu dopadu podľa skutočného stavu v oblasti pôsobnosti príslušných aktív a relevantnosti pre daný scenár rizika.

### Identifikácia existujúcich opatrení

Pri výkone analýzy rizík je potrebné uvažovať aj s existujúcimi implementovanými bezpečnostnými opatreniami. Tieto opatrenia musia byť zohľadnené pri určovaní výslednej hodnoty rizika. Súčasťou identifikácie existujúcich opatrení môže byť pri niektorých analyzovaných rizikách aj popis aktuálneho stavu, resp. zistený nesúlad (s legislatívou, s internými predpismi, atď.).

### Závažnosť rizík

Nasledovná tabuľka popisuje rôzne úrovne závažnosti rizík:

|  |  |
| --- | --- |
| Úroveň závažnosti | Slovný opis závažnosti |
| Mimoriadne vysoké | riziko bezprostredne ohrozuje poskytovanie základnej služby, bezpečnosť organizácie, resp. kritického procesu, alebo systému (typicky prekročenie stanoveného limitu tolerancie rizika, katastrofálna finančná strata alebo škoda na majetku, dopady na zdravie a život, dopad na životné prostredie, atď.) |
| Vysoké | riziko potenciálne ohrozuje poskytovanie základnej služby, bezpečnosť organizácie resp. kritického procesu, alebo systému |
| Nízke | riziko neohrozuje poskytovanie základnej služby, ohrozuje výkon niektorých podporných procesov, kritické procesy, alebo systémy však nie sú rizikom ohrozené |
| Zanedbateľné | riziko neohrozuje poskytovanie základnej služby, výkon procesov a prevádzka systémov nie sú rizikom ohrozené |

## Fázy kvalitatívnej analýzy rizík

Kvalitatívna analýza rizík popísaná v tomto dokumente pozostáva z nasledujúcich fáz:

* identifikácia scenárov rizík,
* vyhodnotenie výsledného rizika pre identifikované hrozby:
* odhad pravdepodobnosti,
* odhad dopadov,
* určenie úrovne závažnosti výsledných rizík.

## Identifikácia scenárov rizík

Scenáre rizík predstavujú špecifické situácie realizácie rizík v kontexte vybraných aktív, pričom môžu byť kombináciou viacerých hrozieb a zraniteľností ústiacimi do rôznych dopadov. Pred samotným výkonom analýzy rizík je potrebné identifikovať všetky podkladové materiály pre popis scenárov rizík, ako sú zoznam aktív a ich vlastníkov, katalóg hrozieb, katalóg zraniteľností. Súčasťou tejto fázy je aj identifikácia existujúcich opatrení pre všetky analyzované oblasti bezpečnosti a súvisiace scenáre rizík.

## Posúdenie rizika kvalitatívnou metódou

Výsledné riziko v identifikovanom scenári sa určuje ako prienik príslušnej hodnoty pravdepodobnosti naplnenia scenára rizika a hodnoty úrovne dopadov, ktoré bude mať na informačné aktíva organizácie.

Pri určovaní týchto hodnôt a pri samotnom vyčíslovaní výsledného rizika sa vychádza aj z úrovne existujúcich opatrení, ktoré môžu mať vplyv na hodnoty pravdepodobnosti či dopadu. Existujúce opatrenia musia byť zahrnuté v popise každého analyzovaného rizika.

Pri určovaní pravdepodobnosti organizácia využíva nasledovnú tabuľku:

|  |  |  |  |
| --- | --- | --- | --- |
| Pravdepodobnosť | % | Frekvencia slovne | Pravdepodobnosť opisne |
| Veľmi nízka | 0-10 | Málokedy | Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľnosti. Neexistuje historická skúsenosť so zneužitím danej zraniteľnosti. |
| Nízka | 11-50 | Niekedy | Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľnosti. Z minulosti existuje ojedinelá skúsenosť zneužitia danej zraniteľnosti. |
| Stredná | 51-80 | Často | Zdroj hrozby je motivovaný a technicky zdatný; uplatnené opatrenia čiastočne bránia úspešnému zneužitiu zraniteľnosti. Existuje skúsenosť z minulosti, že daná zraniteľnost bola už niekoľkokrát zneužitá. |
| Vysoká | 81-100 | Veľmi často | Zdroj hrozby je vysoko motivovaný a je dostatočne technicky zdatný; uplatnené opatrenia na prevenciu identifikovanej zraniteľnosti sú neefektívne. Existuje skúsenosť z minulosti, že daná zraniteľosť bola už mnohokrát zneužitá. |

Pri stanovovaní pravdepodobnosti je potrebné prihliadať aj na frekvenciu výskytu incidentov v minulosti, ktorých podstatou bolo zneužitie príslušnej zraniteľnosti. Ak takýto údaj existuje, mal by byť v súlade so odhadovanou úrovňou pravdepodobnosti.

Pri ohodnocovaní závažnosti dopadov využíva organizácia nasledovnú tabuľku:

| Opis dopadu | Finančný dopad | Prevádzkový dopad | Dopad na súlad | Reputačný dopad |
| --- | --- | --- | --- | --- |
| Zanedbateľný | 1 – 1500 € | Interne, jeden útvar | Zlyhanie interného procesu | Určité prekážky v komunikácií v rámci organizácie |
| Minimálny | 1 501 – 15 000 € | Interne, viacero útvarov | Zlyhanie kritických procesov | Prekážky v komunikácií v rámci organizácie |
| Stredný | 15 001 - 150 000 € | Organizácia, malá časť klientov | Začatie správneho konania smerujúce k opatreniu na nápravu | Závažné prekážky v externej komunikácií |
| Závažný | 150 001 - 1 500 000 € | Organizácia, značná časť klientov | Začatie správneho konania smerujúce k uloženiu pokuty | Nepriaznivá publicita, prípadne na národnej úrovni |
| Katastrofický | 1 500 001 - 15 000 000 € | Organizácia, všetci klienti | Pozastavenie časti služieb / ukončenie činnosti | Intenzívna nepriaznivá publicita na národnej, alebo medzinárodnej úrovni |

## Závažnosť rizika

Výsledné hodnoty množiny je následne možné zaradiť v dvojrozmernej matici:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Pravdepodobnosť scenára rizika** | **Dopad scenára rizika** | | | | |
| **Zanedbateľný** | **Minimálny** | **Stredný** | **Závažný** | **Katastrofický** |
| **Vysoká** | Zanedbateľné | Nízke | Vysoké | Vysoké | Mimoriadne vysoké |
| **Stredná** | Zanedbateľné | Nízke | Nízke | Vysoké | Mimoriadne vysoké |
| **Nízka** | Zanedbateľné | Zanedbateľné | Zanedbateľné | Nízke | Vysoké |
| **Veľmi nízka** | Zanedbateľné | Zanedbateľné | Zanedbateľné | Zanedbateľné | Nízke |

## Návrh bezpečnostných opatrení

Na základe výslednej hodnoty úrovne závažnosti rizika následne organizácia prijíma bezpečnostné opatrenia.

Návrh opatrení v závislosti na stanovenej úrovni závažnosti rizika:

| **Závažnosť rizika** | **Miera rizika** | **Vyhodnotenie** |
| --- | --- | --- |
| A | Mimoriadne vysoké riziko | Rozšírené a dodatočné bezpečnostné opatrenia sú bezpodmienečne nutné a je nutné prijať ich bezodkladne. Výkon kľúčových procesov a ďalšia prevádzka systému je podmienená prijatím opatrní. |
| B | Vysoké riziko | Rozšírené a dodatočné bezpečnostné opatrenia sú potrebné a mali by byť prijaté v dohľadnej dobe, ktorú určí vlastník rizika. Výkon kľúčových procesov organizácie ani prevádzka systému sa nepovažujú za akútne ohrozené. |
| C | Nízke riziko | Vlastník aktíva musí stanoviť, či je nutné prijať rozšírené bezpečnostné opatrenia, alebo či v minulosti prijaté opatrenia sú ešte potrebné. Riziko je možné akceptovať ako prijateľné len v prípade že boli prijaté rozšírené bezpečnostné opatrenia. |
| D | Zanedbateľné riziko | Nie je nutné prijať dodatočné ani rozšírené bezpečnostné opatrenia. Riziko je možné akceptovať ako prijateľné. |

# Výkon analýzy dopadov (BIA)

Analýzou dopadov sa identifikujú rôzne kategórie procesov organizácie, na základe ich kritickosti, ich vzájomné závislosti, analyzujú sa potenciálne dôsledky (škôd/strát) pri rôznych dobách trvania kritických situácií, stanovujú sa cieľové časy obnovy (RTO) a cieľové body obnovy (RPO). Podrobnejšie informácie o analýze dopadov sú popísané v Metodike analýzy rizík a analýzy dopadov zverejnenej na [webovej stránke MIRRI](https://www.mirri.gov.sk/wp-content/uploads/2023/01/KB-K2_3-10-Metodika-na-v%C3%BDkon-anal%C3%BDzy-riz%C3%ADk-v1.1.pdf).

Cieľom analýzy dopadov je najmä:

* zmapovanie organizácie,
* identifikácia závislostí medzi procesmi,
* analýza možných dopadov a určenie RTO a RPO,
* vymedzenie krízových situácii a eliminovanie ich dopadov,
* identifikáciu všetkých zdrojov a prostriedkov nevyhnutných na zabezpečenie kontinuity činností.

## Fázy výkonu analýzy dopadov na činnosti organizácie

Výkon analýzy dopadov je štruktúrovaný do nasledujúcich hlavných fáz:

* úvodné stretnutie k analýze dopadov,
* návrh okruhu procesov a činností, ktoré budú vstupom pre analýzu dopadov,
* moderované workshopy s vlastníkmi príslušných procesov a činností za účelom zberu vstupných údajov pre vykonanie analýzy dopadov,
* realizácia analýzy dopadov,
* vypracovanie správy z analýzy dopadov.

## Zber vstupných dát

Vstupné dáta budú identifikované a analyzované počas moderovaných stretnutí so zodpovednými osobami a kľúčovými zamestnancami odborov a oddelení.

V rámci stretnutia sa vyplní dotazník, ktorý bude po stretnutí zaslaný na verifikáciu a validáciu zodpovedným osobám. Dotazník bude obsahovať nasledovné časti:

* základné informácie o procese,
* väzby a závislosti procesu,
* profil vykonávanej práce,
* funkčné dopady,
* finančné dopady,
* strata údajov
* identifikácia zdrojov a prostriedkov na obnovu procesu
* alternatívny poskytovateľ procesu
* predchádzajúce skúsenosti s krízovými situáciami

Bližší popis údajov, ktoré je potrebné zozbierať v každej časti dotazníka sa nachádza v dokumente „Metodika analýzy rizík a analýzy dopadov“.

## Výstupy z analýzy dopadov

Po zozbieraní všetkých vstupných dát a ich validovaní prebehne finálna analýza dát a ich vyhodnotenie.

Výstupom z analýzy dopadov bude záverečná správa, ktorá bude obsahovať:

* zoznam procesov, ktorý bude (ak to je možné) obsahovať názov procesu, druh procesu, vlastníka procesu, RTO a RPO procesu (údaje, na základe ktorých bolo stanovené príslušné RTO a RPO budú taktiež súčasťou správy),
* špecifikácie nevyhnutných zdrojov a prostriedkov pre zabezpečenie kontinuity činností.

### Stanovenie hodnôt RTO a RPO

Stanovenie hodnoty RTO

RTO procesu sa určí podľa už stanoveného MTO príslušnej činnosti s prihliadnutím na závislosti medzi procesmi.

RTO procesu sa musí oproti MTO príslušnej činnosti ponížiť, ak na procese je závislý iný proces, ktorého stanovená hodnota RTO je nižšia než príslušné MTO.

RTO pre informačné systémy, aplikácie a databázy sa určí ako minimálne RTO všetkých procesov, ktoré sú závislé na danom informačnom systéme, aplikácii a databáze.

Stanovenie hodnoty RPO

RPO procesu sa určí analyticky na také časové obdobie, ktoré zodpovedá hranici medzi akceptovateľnými a neakceptovateľnými dopadmi straty údajov pre všetky typy údajov.

RPO pre informačné systémy, aplikácie a databázy sa určí analyticky na také časové obdobie, ktoré zodpovedá hranici medzi akceptovateľnými a neakceptovateľnými dopadmi straty údajov, ktoré sú uchovávané v aplikáciách a databázach.