NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Metodika analýzy rizík kybernetickej bezpečnosti

Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Verzia	2.0
Dátum vydania	01.09.2025
Dátum účinnosti	01.09.2025

Národný bezpečnostný úrad | Budatínska 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | podatelna@nbu.gov.sk | www.nbu.gov.sk

Obsah

1. Úvod

1.1. Riadenie rizika

Informačné aktíva pre väčšinu organizácií predstavujú súčasnú, alebo potenciálnu hodnotu. Od ich dostupnosti, integrity a dôvernosti závisí kvalita poskytovaných služieb a schopnosť organizácie efektívne dosahovať svoje ciele. Z tohto dôvodu musia byť primeraným spôsobom chránené. Bezpečnosť informačných aktív je založená na udržiavaní akceptovateľnej miery identifikovaného rizika prostredníctvom komplexných procesov a činností zameraných na odvrátenie, alebo zmenšenie identifikovaných rizík, resp. prejavov a následkov hrozieb, ktoré pôsobia na informačné aktíva.

Podľa všeobecnej definície je riziko chápané ako „vplyv neistoty na ciele“. Pre potreby tohto dokumentu sú kybernetické bezpečnostné riziká definované ako: „**riziká budúcich priamych finančných a nepriamych (napr. reputačných) strát spôsobených narušením dôvernosti, integrity, dostupnosti, alebo sledovateľnosti informačných aktív organizácie, vytvorených, uložených, spracúvaných, alebo prenášaných informačnými a komunikačnými technológiami**“. Termín „kybernetické bezpečnostné riziko“ je tiež ekvivalentom výrazu „IT riziko“.

1.2. Význam metodiky riadenia rizika

Cieľom tohto dokumentu je poskytnúť návody a usmernenia o postupoch súvisiacich s riadením kybernetických bezpečnostných rizík pre prevádzkovateľov základných služieb, ako povinné osoby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov ďalej len „zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti“).

1.3. Zásady navrhovanej metodiky

Analýza rizík má slúžiť k podrobnému rozboru stavu kybernetickej a informačnej bezpečnosti v organizácii. Cieľom analýzy rizík má byť identifikácia, analýza a evaluácia okolností, ktoré potenciálne môžu narušiť bezpečnosť (t. j. hrozieb, zraniteľností, scenárov rizík a škodlivých udalostí).

Základnou zásadou tejto metodiky je **všeobecná použiteľnosť**. Autori zohľadnili viaceré technické normy a metodiky riadenia rizík s cieľom dosiahnuť univerzálnu aplikovateľnosť naprieč odvetviami, nezávisle od vyspelosti jestvujúcich procesov riadenia rizík u prevádzkovateľa. **Pokiaľ má prevádzkovateľ implementovaný proces riadenia rizík s vyššou úrovňou vyspelosti, uplatňuje sa existujúci prístup prevádzkovateľa**.[1]

Materializáciou rizík vznikajú bezpečnostné incidenty. Pre štatistické účely a pre potreby oznamovania kybernetických bezpečnostných incidentov Národný bezpečnostný úrad (ďalej len „úrad“) **stanoví jednotnú metriku**. Pokiaľ má prevádzkovateľ základných služieb implementovaný proces riadenia rizík s vyššou úrovňou vyspelosti, rozdielny od tejto metodiky, navrhne spôsob mapovania hodnôt z používanej metriky na požadovanú jednotnú metriku podľa tejto metodiky.

Výsledkom analýzy rizík musí byť ohodnotený (evaluovaný) zoznam identifikovaných scenárov rizík a návrh bezpečnostných opatrení, ktoré slúžia na ošetrenie významných rizík.

Preferovanou metódou ošetrovania rizika má byť redukcia rizika na akceptovateľnú úroveň. Riziká majú byť primárne ošetrované v poradí od najvyššej závažnosti po najnižšiu.

Analýza rizík musí byť vykonaná v takom detaile, ktorý umožní určiť, či je zvyškové riziko akceptovateľné (t. j. či hodnota zvyškového rizika je na zanedbateľnej úrovni).

[1] To však nesmie byť v rozpore so sektorovo špecifickými požiadavkami a metodickými postupmi v oblasti analýzy a riadenia rizík

Odhad pravdepodobnosti zohľadňuje najpravdepodobnejšiu kombináciu hrozieb, poprípade odhadovanú, či odmeranú početnosť výskytu daného konkrétneho scenára v uvažovanej populácii (referenčnej skupine/triede), v ktorej je následne priradená slovná, alebo číselná hodnota pravdepodobnosti, v rámci stanovenej metriky.

Odhad závažnosti potenciálnych následkov zohľadňuje najhorší možný následok hrozieb, resp. hornú hranicu intervalového odhadu škôd v konkrétnom scenári, ktorému je následne priradená slovná, alebo číselná hodnota závažnosti následku, v rámci stanovenej metriky.

Vyhodnotenie výsledného aktuálneho rizika (current risk) je vyjadrené ako kombinácia odhadu pravdepodobnosti a odhadu závažnosti následkov plynúcich z možného naplnenia hrozby, škodlivej udalosti, alebo kombinácie hrozieb, po zohľadnení existujúcich bezpečnostných opatrení, to znamená po zohľadnení daného konkrétneho scenára hodnoteného pre aktuálnu sadu bezpečnostných opatrení (current baseline).

Identifikované zraniteľnosti, hrozby, potenciálne škodlivé udalosti sú sumarizované do konkrétnych scenárov rizík, v kontexte príslušného informačného aktíva. Scenáre rizík sú často orientované na analýzu a rizikovosť konkrétneho biznis procesu, ktorý sa skladá z jednotlivých informačných aktív.

Pre riziká týkajúce sa okolia, na ktoré v rámci analýzy rizík konkrétneho aktíva nie je dosah, sú bezpečnostné opatrenia popísané formou požiadaviek, resp. odporúčaní na okolie.

Analýza rizík spĺňa požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti..

1.4. Právny základ a normatívne odkazy

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

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach
- ISO/IEC 27000:2018 Informačné technológie – Bezpečnostné metódy – Systém riadenia informačnej bezpečnosti – Prehľad a slovník
- STN ISO/IEC 27005:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia – Usmernenie k riadeniu rizík informačnej bezpečnosti
- ISO 31000:2018 Manažérstvo rizika – Návod
- ISO 31010:2019 (Risk assessment techniques)
- NIST Special Publication 800-39 Managing Information Security Risk
- NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments
- Open Group Standard (Open FAIR Body of Knowledge – O-RA & O-RT, ed. C20:2019)

Pokiaľ nie je uvedená verzia dokumentu, všetky vyššie uvedené právne predpisy a technické normy sú citované v znení ich platnej verzie. Relevantné časti tejto metodiky sa opierajú aj o ustanovenia osobitných predpisov.[2]

[2] Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

1.5. Definície a kľúčové pojmy

Pojem	Skratka	Výklad
aktívum		hmotný alebo nehmotný komponent informačnej architektúry, ktorý má pre prevádzkovateľa základnej služby hodnotu, najmä služby, procesy, informácie alebo údaje
analýza rizík		proces na pochopenie pôvodu rizík a zistenie úrovne rizík; analýza rizík poskytuje základ na vyhodnotenie rizík a rozhodnutie o spôsobe ich ošetrenia
kybernetická bezpečnosť		stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov
riziko		potenciál straty alebo narušenia v dôsledku kybernetického bezpečnostného incidentu vyjadrený ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu kybernetického bezpečnostného incidentu
kybernetický bezpečnostný incident		udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov
hrozba		akákoľvek okolnosť či udalosť, ktorá môže potenciálne využiť zraniteľné miesto informačných, alebo fyzických aktív a spôsobiť negatívny následok
kybernetickou hrozbou		kybernetická hrozba podľa čl. 2 bodu 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (ďalej len „nariadenie (EÚ) 2019/881“)
informačné aktíva		všetky objekty, komponenty podieľajúce sa na dodávke IT produktov, alebo IT služieb, ktoré pre organizáciu priamo, alebo nepriamo predstavujú súčasnú, alebo potenciálnu hodnotu, alebo ktorých narušenie integrity, dôvernosti a dostupnosti môže mať na organizáciu negatívny následok
kybernetická odolnosť		schopnosť organizácie kontinuálne pokračovať v činnosti s najmenšou mierou narušenia aj v prípade kybernetického bezpečnostného incidentu, alebo inej škodlivej udalosti

Pojem	Skratka	Výklad
kybernetické bezpečnostné riziko		riziko spôsobené narušením dôvernosti, integrity, dostupnosti, alebo sledovateľnosti informačných aktív organizácie, vytvorených, uložených, spracúvaných, alebo prenášaných informačnými technológiami
následok		hodnota závažnosti ujmy, resp. rozsah škody, ktorá môže byť spôsobená zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou
ochrana		starostlivosť o odvrátenie nebezpečenstva; prostriedok na chránenie; prevencia - súhrn opatrení na odvrátenie, alebo zmiernenie škodlivých vplyvov a následkov incidentov, mimoriadnych udalostí a krízových situácií
organizačné opatrenia		systém administratívnych pravidiel, ktoré vymedzujú pravidlá správania sa zamestnancov a tretích strán v súvislosti s ochranou fyzických a informačných aktív
ošetrenie rizika		proces modifikácie/zvládnutia rizika (typicky implementácia opatrení pre zníženie rizika)
používateľ		osoba, ktorá spracúva (najmä vytvára, používa, mení, premiestňuje) informačné aktíva organizácie v preddefinovaných procedúrach počas vykonávania pridelených úloh – špecificky zamestnanec organizácie, alebo zamestnanec tretej strany
riadenie rizík		koordinované aktivity na riadenie organizácie s ohľadom na riziká
riešenie bezpečnostných incidentov		aktivita a postup zamerané na prevenciu, odhaľovanie, analýzu a obmedzovanie kybernetického bezpečnostného incidentu alebo na reakciu naň a zotavenie z neho
riziko		pravdepodobnosť, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho následku, alebo škody
rizikový apetít		ochota organizácie prijať (tolerovať) riziká tak, ako sú popísané či kvantifikované príslušnými ukazovateľmi
scenár rizika		sled alebo kombinácia udalostí vedúcich od počiatočnej príčiny k nežiaducemu následku
tolerancia rizika		miera, do akej organizácia vyžaduje, aby boli jej informačné aktíva chránené pred hrozbami
úroveň rizika		závažnosť rizika vyjadrená ako výsledný očakávaný efekt možných následkov a ich pravdepodobnosti, produkt odhadu pravdepodobnosti a odhadu možných závažností následkov
vlastník rizika		osoba zodpovedná za monitorovanie a riadenie všetkých aspektov konkrétneho rizika, ktoré mu bolo pridelené, vrátane implementácie vybraných opatrení určených pre odstránenie alebo minimalizovanie hrozby

Pojem	Skratka	Výklad
zraniteľnosť		akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou

2. Proces riadenia rizika

Proces riadenia rizika pozostáva z cyklických a na seba nadväzujúcich procesov:

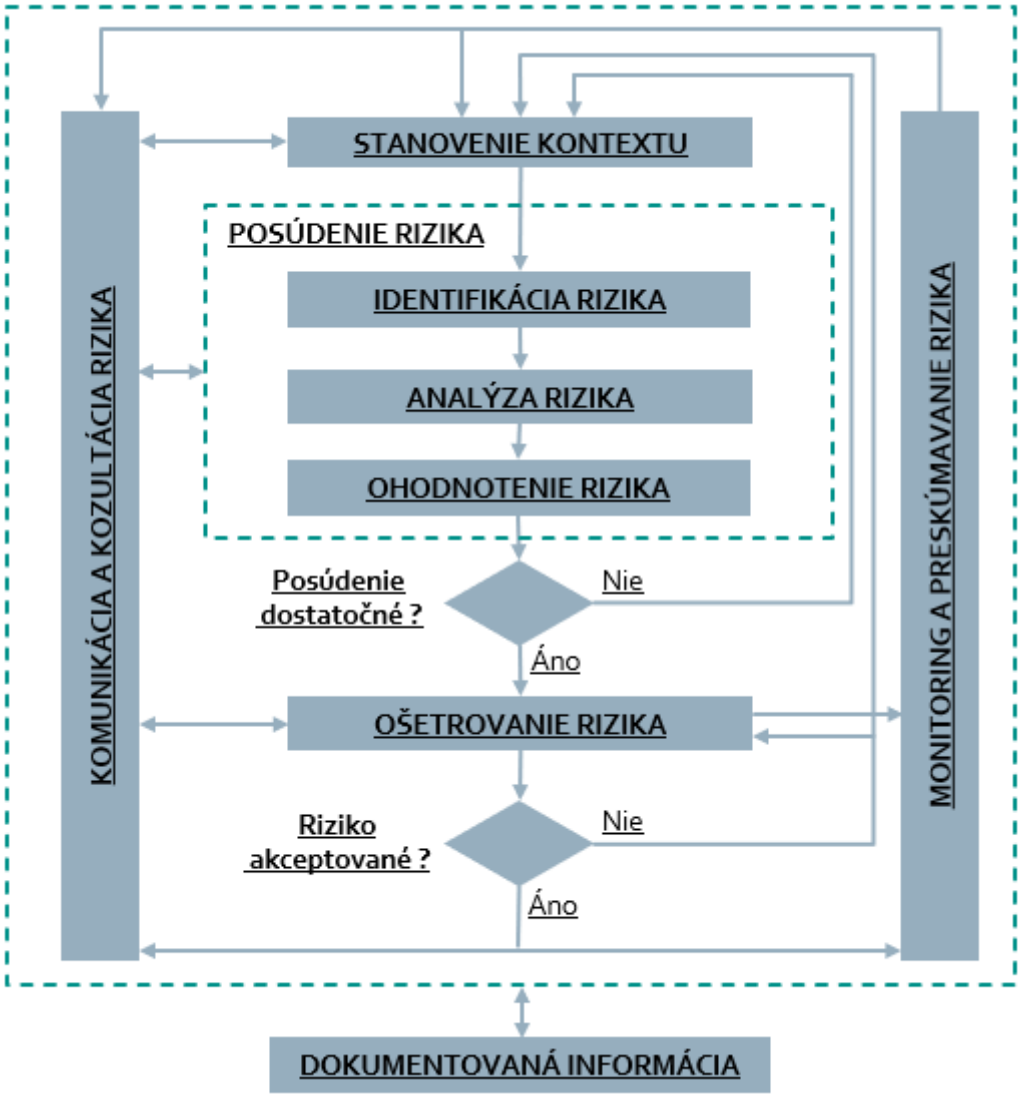
1. stanovenie kontextu rizík
2. posúdenie rizík
3. ošetrovanie rizík
4. komunikácia o rizikách
5. monitorovanie a preskúmanie rizík

Posúdenie rizík (2) je komplexný proces, ktorý pozostáva z:

1. identifikácie rizík,
2. analýzy rizík a
3. ohodnotenia rizík.

S cieľom zjednodušenia názvoslovia sa v tejto metodike ďalej namiesto výrazu „posúdenie rizika“ používa len súhrnný výraz „**analýza rizika**“.

Všeobecná schéma procesu riadenia rizík informačnej bezpečnosti podľa STN ISO/IEC 27005:2023


STANOVENIE KONTEXTU
POSÚDENIE RIZIKA
IDENTIFIKÁCIA RIZIKA
ANALÝZA RIZIKA
OHODNOTENIE RIZIKA
Posúdenie dostatočné ?
Nie
Áno
OŠETROVANIE RIZIKA
Riziko akceptované ?
Nie
Áno
KOMUNIKÁCIA A KOZULTÁCIA RIZIKA
MONITORING A PRESKÚMAVANIE RIZIKA
DOKUMENTOVANÁ INFORMÁCIA

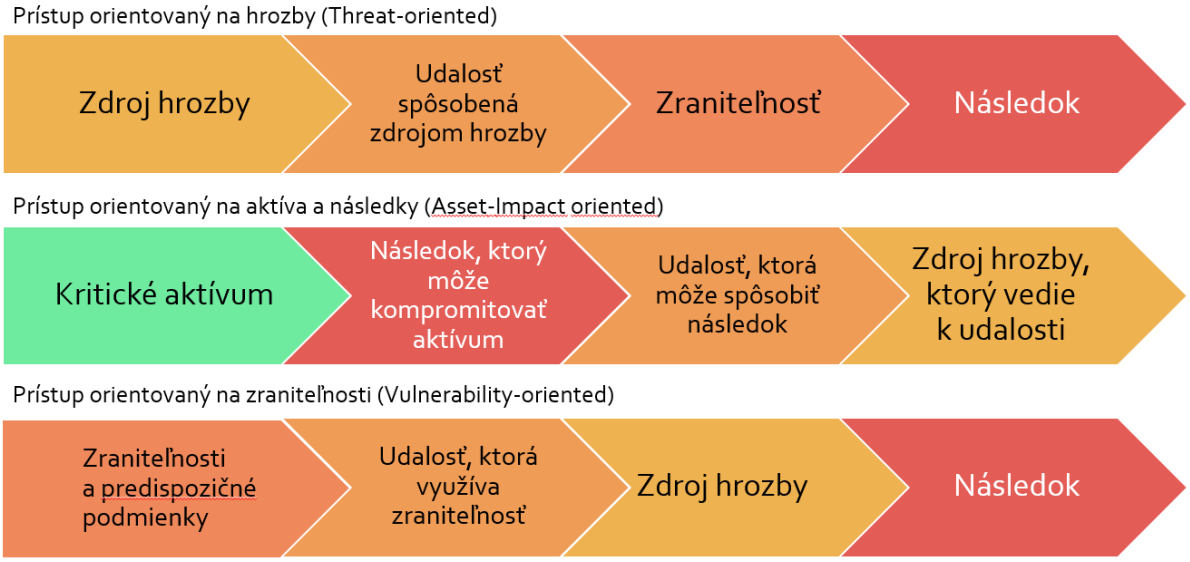
3. Metodika analýzy rizík

3.1. Prístupy k analýze rizika

Podľa NIST SP 800-39, NIST SP 800-30[3] existujú tri rôzne prístupy k analýze rizika s rôznymi výhodami a rôznou zložitosťou:

- **Prístup orientovaný na hrozby** (z angl. Threat oriented)
  - Identifikuje zdroje hrozieb a udalosti
  - Umožňuje rozvinúť scenáre a modely hrozieb
  - Identifikuje zraniteľnosti v kontexte hrozieb
- **Prístup orientovaný na aktíva a následky** (z angl. Asset-Impact oriented)
  - Identifikuje aktíva kritické pre činnosti (z angl. business critical / mission critical)
  - Umožňuje analýzu dôsledkov hrozieb a udalostí
  - Identifikuje zraniteľnosti voči udalostiam ohrozenia kritických aktív so závažným nepriaznivým vplyvom
- **Prístup orientovaný na zraniteľnosti** (z angl. Vulnerability-oriented)
  - Identifikuje predispozičné podmienky
  - Identifikujte zneužiteľné zraniteľnosti
  - Identifikujte hrozby v kontexte známych/identifikovaných zraniteľností

Rozdiely v postupnosti procesu analýzy rizika v rámci týchto prístupov je možné zobraziť graficky:



[3] NIST Special Publication 800-39 Managing Information Security Risk, NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments

3.2. Metódy hodnotenia rizika

Metóda	Popis	Výhody	Nevýhody
Kvalitatívna	Hodnotenie rizík pomocou slovných opisov alebo škál	Rýchla, jednoduchá, vhodná pri menej vyspelom riadení rizík	Určitá miera subjektivity, obmedzená presnosť
Kvantitatívna	Číselné vyjadrenie rizík pomocou dát a výpočtov	Vysoká presnosť, umožňuje finančné modelovanie	Náročná na dáta a výpočty
Semikvantitatívna	Kombinuje slovné hodnotenie s číselnými stupnicami	Vyvážená presnosť, ľahšia interpretácia, vhodná pre tímovú prácu	Určitá miera subjektivity, obmedzená presnosť

3.2.1. Kvalitatívne metódy

Na definovanie rizikových faktorov sú použité **nečíselné (slovné) hodnoty.** Miera pravdepodobnosti a následku je určená na základe individuálnych odborných znalostí. Takéto vyjadrenie jednotlivých udalostí využíva odhad, ktorý vyjadruje mieru osobného presvedčenia o výskyte posudzovaného javu (hrozby, škodlivej udalosti). Slovná deskripcia pravdepodobnosti je pre väčšinu používateľov zrozumiteľnejšia a prijateľnejšia. Prioritizácia rizík na ich postupné zvládanie prebieha subjektívne na základe bodového hodnotenia alebo farebného označenia.

Kvalitatívne metódy sa využívajú v prípadoch, ak chýbajú, alebo sú ťažko vyjadriteľné číselné hodnoty pre kvantitatívne ohodnotenie rizika. Sú vhodné pre organizácie s menej vyspelými procesmi riadenia rizík. Ako základné pre rýchlu analýzu rizík, tvoria základný, štartovací bod pre riadenie rizík.

3.2.2. Kvantitatívne metódy

Rizikové faktory sa používajú na určenie (výpočet) miery pravdepodobnosti a miery možnej straty v merateľných jednotkách (typicky anualizovaná pravdepodobnosť alebo ročná frekvencia výskytu daného rizikového scenára a výška straty vo finančných jednotkách).

Parametre (zložky) rizika, najmä zložka následkov/strát, nie sú vyjadrené bodovými (diskrétnymi) hodnotami, ale intervalovými odhadmi s príslušným štatistickým rozdelením možných hodnôt (typicky horná hranica, stredná hodnota a dolná hranica na pravdepodobnostnej distribučnej funkcii pre možné veľkosti následku daného rizikového scenára). Intervaly vyjadrujú tak štatistickú (prirodzenú) mieru neurčitosti, ako aj odhadovanú mieru neistoty pri určení daného parametra.

Na určenie intervalových odhadov sa používajú buď individuálne odborné znalosti kalibrovaných expertov (podobne ako pri kvalitatívnych metódach), alebo vhodné štatistiky a historické údaje (relevantné pre daný scenár, populáciu alebo referenčnú skupinu), prípadne výpočty zohľadňujúce subjektívne názory aj objektívne dôkazy.[i]

Výsledkom kvantitatívneho hodnotenia pravdepodobnosti a následkov je krivka, typicky krivka prekročenia strát (LEC, CCDF) alebo hodnota ohrozená rizikom (VaR, CDF).

Prioritizácia rizík na ich postupné zvládanie prebieha na základe objektívnych informácií (odhadov), vrátane porovnania výsledkov s krivkou tolerovaného rizika (RTC), ekonomických kalkulácií návratnosti investícií do bezpečnostných opatrení (RoC, ROSI) a ekonomicky optimálnej skladby opatrení.

Individuálne výsledky (krivky) je možné agregovať podľa typov scenárov, typov dotknutých aktív alebo typu narušenia do miery rizika v čiastkovom portfóliu (ľudský faktor, živelné udalosti, cloud, dátové centrum, aplikácie, strata dôvernosti) alebo do celkovej miery expozície voči kybernetickým rizikám.

Kvantitatívne metódy sa využívajú v prípadoch, keď má organizácia povinnosť alebo obchodný záujem používať pokročilejšie, presnejšie a dôveryhodnejšie metódy práce s rizikami, alebo keď existuje

na úrovni vedenia spoločnosti ambícia riadiť rozhodnutia a investície do kybernetickej bezpečnosti na základe ekonomických ukazovateľov a objektívnych informácií a dát.

Kvantitatívne metódy sú v tomto prípade chápané ako pokročilé metódy riadenia rizík, ktoré prinášajú naviac možnosť ekonomického vyhodnotenia investícií do opatrení, možnosť čisto ekonomickej alebo strategicko-ekonomickej optimalizácie plánu rozvoja kybernetickej bezpečnosti, možnosť porovnania rôznych zvažovaných bezpečnostných opatrení.

3.2.3. Semikvantitatívne (zmiešané) metódy

Na definovanie rizikových faktorov sa používajú číselné hodnoty (niekedy v spojení so slovným hodnotením), prípadne číselné rozsahy hodnôt so slovne vyjadreným kontextom. Hodnoty pravdepodobnosti a následku sú odvodené z rozsahu číselnej stupnice s priradením príslušného stupňa jedinečného významu. Výsledkom semikvantitatívneho hodnotenia pravdepodobnosti a následkov je bod v matici s vyjadrenou mierou pravdepodobnosti a mierou dopadu (t. j. škály umožňujú jednoznačný prevod hodnôt na pravdepodobnosť a následok).

Tieto metódy sa využívajú najmä v oblasti prioritizácie bezpečnostných rizík, t. j. pri určovaní správnej a zdôvodnenej priority bezpečnostných rizík.

3.2.4. Použitá metóda

Analýzu rizika je možné vykonať v rôznej miere detailu v závislosti od dôležitosti (kritickosti) aktív, rozsahu známych zraniteľností a predchádzajúcich incidentov, s ktorými sa organizácia v minulosti stretla.

Analýza rizík vykonaná podľa tejto metodiky je založená na **kvalitatívnej,** alebo **semikvantitatívnej** alebo **kvantitatívnej** analýza, v závislosti od legislatívnych požiadaviek,[4] podľa bezpečnostných štandardov[5] a potrieb organizácie.[6]

[4] Vyhláška UPVII č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy ako aj Vyhláška NBÚ č. 272/2025 Z. z., o bezpečnostných opatreniach

[5] STN ISO/IEC 27005:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia – Usmernenie k riadeniu rizík informačnej bezpečnosti

[6] napr. Metodika analýzy bezpečnosti pre bezpečnostné projekty ISVS vydaná Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky v roku 2024

4. Stanovenie kontextu rizika

V rámci stanovenia kontextu organizácia definuje vonkajšie a vnútorné parametre, ktoré je potrebné vziať do úvahy pri riadení rizika, a stanovuje rozsah a kritériá rizika pre samotný proces. Aj keď mnohé z týchto parametrov sú podobné tým, ktoré sa zvažujú pri navrhovaní rámca riadenia rizík, pri stanovovaní kontextu procesu riadenia rizík je potrebné ich zvážiť podrobnejšie a najmä to, ako súvisia s rozsahom konkrétneho riadenia rizík.

Stanovenie kontextu pozostáva najmä z nasledujúcich činností:

a) identifikácia aktív a ich vlastníkov,
b) identifikácia zraniteľností,
c) identifikácia potenciálnych hrozieb,
d) odhad následkov,
e) odhad pravdepodobností,
f) identifikácia existujúcich opatrení.

4.1. Identifikácia aktív a ich vlastníkov

Jednou zo základných úloh manažmentu je riadenie zdrojov, do ktorej patrí aj ochrana aktív. Hlavným cieľom riadenia kybernetickej bezpečnosti je zabezpečiť ochranu aktív v súlade s ich hodnotou. Pri ochrane aktív a prijímaní bezpečnostných opatrení sa preto musí prihliadať na ich súčasnú, alebo potenciálnu hodnotu.

Prvým krokom pri ochrane aktív je vytvorenie prehľadného zoznamu aktív a ich vlastníkov, ktorý je jedným z hlavných vstupov do analýzy rizík. Aktíva musia byť identifikované a inventár týchto aktív musí byť zaznamenaný a riadený. Zoznam aktív môže byť rozdelený do typov aktív. Navrhované typy aktív sú uvedené v Prílohe č. 3.

Procesy riadenia aktív by mali obsahovať identifikáciu a evidenciu všetkých:

a) primárnych aktív,
b) podporných aktív,
c) vlastníkov aktív,
d) zodpovedných osôb za identifikáciu a evidenciu aktív.

Na podporné aktíva tvoriace hranicu medzi aktívami s rozdielnou hodnotou sa prihliada ako na aktíva s najvyššou hodnotou z príslušných aktív. Na podporné aktíva, ktoré pomáhajú funkciám primárnych aktív, sa prihliada ako na aktíva s najvyššou hodnotou zo súvisiacich primárnych aktív.

Za tvorbu a prispievanie do zoznamu aktív a zoznamu rizík je zodpovedný **vlastník rizika**, t. j. osoba zodpovedná za monitorovanie a riadenie všetkých aspektov konkrétneho rizika, ktoré mu bolo pridelené, vrátane implementácie vybraných opatrení určených pre hrozby, alebo na maximalizáciu príležitostí. Organizácia by mala zaviesť mechanizmy komunikácie rizika, s cieľom podporiť zodpovednosť a vlastníctvo rizika. Tieto mechanizmy by mali zabezpečiť, aby kľúčové komponenty rizika v rámci procesov riadenia rizík boli primerane a včas komunikované zo všetkými zainteresovanými stranami.

V rámci identifikácie aktív by mal byť vytvorený katalóg, ktorý popisuje všetky relevantné aktíva. Vytvorenie zoznamu aktív, je vo väčších organizáciách súčasťou procesu riadenia aktív (z angl. „Asset management“). Na definícii kritickosti aktív sa významne podieľa aj analýza funkčných dopadov (z angl. „Business Impact Analysis“ – BIA), ako špecifická analýza rizík pôsobiacich najmä na dostupnosť, ktorá je vykonávaná v rámci procesov riadenia kontinuity činností (z angl. Business Continuity

Management“ - BCM). Popis týchto dvoch procesov nie je predmetom tejto metodiky a čitateľovi je odporúčané vyhľadať príslušné zdroje.

Podľa potreby môžu byť informačné aktíva logicky usporiadané do hierarchickej štruktúry pre zefektívnenie odkazovania sa na konkrétne aktíva v rámci celej analýzy rizík. Jedným z možných prístupov je použitie tzv. Rasmussenovej abstraktnej hierarchie.[7] Táto technika umožňuje rozhodnúť o tom, aký detail sa použije pre usporiadanie informačných aktív a následne na aké komponenty informačnej architektúry organizácie bude orientované posudzovanie rizika.

Rasmussenova hierarchia komponentov informačnej architektúry:

Podrobnejší popis vhodnosti použitia analýzy rizík podľa dvoch rôznych pohľadov podľa Rasmussena je v nasledujúcej tabuľke:

Posúdenie rizika	Použitie
Komponentovo orientované	• Analýza rizika v kontexte konkrétnych komponentov architektúry • Dekompozícia menej komplexných systémov, s dobre zmapovanými prepojeniami medzi komponentami architektúry • Spracovanie na úrovni abstrakcie, kde fyzické funkcie sú odsúhlasené zainteresovanými stranami
Systémové orientované	• Skúmanie hrozieb, v rámci komplexnej interakcie mnohých častí systému • Stanovenie požiadaviek na bezpečnosť systému skôr, ako sa rozhodnete pre konkrétny návrh architektúry systému • Zhrnutie spoločného pohľadu viacerých zainteresovaných strán na to, čo by systém mal a čo nemal poskytovať (napr. bezpečnosť, výkon, súlad) • Analýza hrozieb, ktoré nie je možné preskúmať do úrovne jednotného bodu zlyhania

Dá sa zjednodušene tvrdiť, že pre väčšie organizácie je vhodnejšie systémovo orientované, vysokoúrovňové posudzovanie rizík a **konceptuálny pohľad** cez účely (t. j. procesy, určenie informačných systémov), zatiaľ čo pre malé organizácie je efektívnejšie komponentovo orientované, detailné posudzovanie rizík a pohľad cez **reálne formy** a funkcie komponentov (t. j. zariadenia, fyzické lokality, aplikácie).

[7] Jens Rasmussen: Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering, September 1986, ISBN:978-0-444-00987-6, 228 str.

4.2. 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.

Pre efektívne riadenie rizík je nevyhnutné identifikovať všetky hrozby spôsobilé narušiť informačnú a kybernetickú bezpečnosť. Zoznam uvažovaných hrozieb je potrebné uviesť v Katalógu hrozieb.

Katalóg hrozieb napomáha identifikácii hrozieb využitím existujúcej taxonómie a poskytuje zoznam všetkých dôvodne očakávaných hrozieb v organizácii. Generický katalóg hrozieb je účelné doplniť o ďalšie, najmä špecifické hrozby. Pri tvorbe katalógu by sa mali vziať do úvahy skúsenosti z incidentov a hrozieb ktoré sa stali v minulosti.

Pre potreby analýzy rizík sa zoznam hrozieb združuje do jednotlivých skupín tak, že je možné tento zoznam použiť univerzálne pre väčšinu aktív. **Pre jednotlivé aktíva sú hodnotené len hrozby relevantné pre konkrétne aktívum**.

Hrozby sa v katalógu rozdeľujú podľa ich pôvodu do kategórií najmenej ako:

- Úmyselné hrozby pre všetky úmyselné aktivity zamerané na aktíva,
- Náhodné hrozby pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť aktíva,
- Hrozby spôsobené vplyvom prostredia pre všetky udalosti, ktoré vznikajú nezávisle od ľudskej činnosti.

Zdrojom 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.

4.2.1. Verejné katalógy hrozieb

- Verejný katalóg hrozieb Národného bezpečnostného úradu SR – poskytuje viac ako 100 hrozieb v 15 kategóriách vybraných z nižšie uvedených katalógov, vrátane popisu, resp. typického príkladu a vplyvu hrozby na atribúty dôvernosti, integrity a dostupnosti
- Katalóg National Institute of Standards & Technology (NIST) SP 800-30 – poskytuje návrh približne 100 typických škodlivých udalostí
- Katalóg ENISA Threat Taxonomy – poskytuje klasifikáciu hrozieb a približne 170 typov hrozieb na rôznej úrovni detailu
- ENISA Interoperable EU Risk Management Toolbox – poskytuje katalóg 70 typov hrozieb v 5 kategóriách, vrátane ich väzby na bezpečnostné atribúty a kategórie podporných aktív
- STN ISO/IEC 27005:2023 – poskytuje príklad katalógu 57 hrozieb v 7 kategóriách
- Bundesamt für Sicherheit in der Informationstechnik (BSI) IT- Grundschutz-Katalog – poskytuje komplexný zoznam 370 hrozieb spolu s príkladmi pre každú z nich

4.2.2. Zdroje dodatočných informácií o hrozbách

Okrem externých, verejných katalógov hrozieb môžu byť relevantné najmä nasledujúce dodatočné zdroje informácií:

- Výkonní zamestnanci – osobne, mailom, telefonicky, príp. prostredníctvom rôznych formulárov alebo systému ServiceDesk, ak je implementovaný
- Odborní zamestnanci – riziká zistené náhodne, alebo ako výsledok analýz v procese štandardnej prevádzky informačných systémov, ktoré môžu identifikovať najmä zamestnanci IT alebo v rámci práce Operačného centra kybernetickej bezpečnosti (Security operations center).

- Procesy riadenia IT služieb - riziká zistené pri nahlásení incidentu, alebo iného typu požiadavky na ServiceDesk, ktoré môžu identifikovať najmä zamestnanci IT a útvarov bezpečnosti.
- Analýza funkčných dopadov (BIA) – výstupom analýzy funkčných dopadov je register procesov a hodnotenia ich kritickosti z pohľadu zaručenia kontinuity činností, t. j. najmä pre atribút dostupnosti
- Testovacie procesy – testovanie softvéru, penetračné testy a iné typy posudzovania a analýzy zraniteľností
- Výsledky analýz rizík a bezpečnostných testov vykonávaných v rámci plánu testovania, alebo náhodne
- Projektový manažment - projektoví manažéri a projektové tímy – najmä identifikované riziká IT projektov
- Odporúčania auditu – riziká a hrozby identifikované v rámci programu interného auditu, alebo zistenia nesúladu konštatované certifikovaným audítorom kybernetickej bezpečnosti
- Monitoring - výstupy automatizovaných monitorovacích systémov prevádzky, resp. bezpečnosti
- Incidenty - záverečné správy o incidentoch, t. j. výstupy poučenia z uskutočneného incidentu
- Tretie strany - notifikácia od externej osoby resp. organizácie, ktorá je akýmkoľvek spôsobom informovaná o riziku (napr. výrobcovia HW a SW, dodávatelia služieb, konzultačné spoločnosti, klienti, webové fóra, blogy, mailinglisty, atď.)

4.3. Identifikácia zraniteľností

Zraniteľnosť je takým miestom v prostredí IS resp. organizácie, ktoré má potenciál byť zneužité hrozbou a spôsobiť negatívny následok na informačné aktíva organizácie, alebo organizáciu ako celok. V rámci analýzy rizík sú identifikované zraniteľnosti, ktoré môžu byť využité hrozbami na spôsobenie škody na identifikovaných aktívach.

Identifikáciu uvažovaných zraniteľností je vhodné udržiavať v **Katalógu hrozieb**, resp. v samostatnom **Katalógu zraniteľností**. Pre rozsiahlejšie prostredia je vhodné použiť niektorý zo softvérových nástrojov pre riadenie rizika. Tieto typicky obsahujú aj funkcionality katalógu hrozieb a zraniteľností.

4.4. Odhad následkov

Identifikované typy následkov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti je vhodné uviesť v zozname typov následkov.

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

Pri použití kvantitatívnych metód sa spolu s typmi následkov (relevantnými pre daný scenár) určuje aj ich intenzita a nákladový faktor (t. j. prevod straty na peňažné jednotky, napr. strata za jednu hodinu výpadku/nedostupnosti v EUR).

4.5. Odhad pravdepodobností

Určenie pravdepodobnosti naplnenia scenára rizika je požiadavkou na vyhodnotenie daného scenára rizika. Pri kvalitatívnom a semikvantitatívnom riadení rizík je potrebné mať na pamäti, že riziko s veľkým následkom, ktoré sa však vyskytne iba raz za dlhý časový horizont môže mať menší negatívny vplyv na bezpečnosť ako riziko s nízkym následkom, avšak s častejším výskytom. Poznať, resp. správne odhadnúť pravdepodobnosť výskytu je preto dôležitou súčasťou hodnotenia výsledného rizika. Do výslednej hodnoty pravdepodobnosti musia byť zohľadňované aj existujúce bezpečnostné opatrenia súvisiace s daným scenárom rizika.

Na určenie celkovej pravdepodobnosti, ktorá naznačuje šancu, že potenciálna zraniteľnosť môže byť zneužitá v rámci existujúcej infraštruktúry a prostredia, musia byť zvážené nasledujúce faktory:

- motivácia a zdatnosť zdroja hrozby,
- podstata zraniteľnosti,
- existencia a efektivita aktuálne uplatnených opatrení.

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 stanovenou úrovňou pravdepodobnosti.

Pri použití kvantitatívnych metód sa na odhad pravdepodobnosti používa koncept referenčnej triedy (skupiny), t. j. v koľkých prípadoch (absolútne) alebo v akom percente členov (relatívne) skupiny daná situácia nastala počas definovaného obdobia.

4.6. Identifikácia existujúcich bezpečnostných opatrení

Pri výkone analýzy rizík je prostredie organizácie, resp. nasadenia / prevádzky IS skúmané ako jeden celok, vrátane existujúcich bezpečnostných opatrení. Tieto musia byť zohľadnené pri určovaní výslednej hodnoty rizika. Identifikácia a popis existujúcich bezpečnostných opatrení majú byť vykonané pre každé analyzované riziko, príp. spoločne pre celú oblasť bezpečnosti s následnou referenciou relevantných existujúcich opatrení v každom súvisiacom riziku.

Popri identifikácii existujúcich opatrení sa zároveň overuje, či implementované opatrenia fungujú správne, ak opatrenia nefungujú podľa očakávania, môžu samé o sebe vyvolať zraniteľnosť. Súčasťou identifikácie existujúcich opatrení môže byť pri niektorých analyzovaných rizikách aj popis aktuálneho stavu, resp. zistený nesúlad (s legislatívou, s internými predpismi, atď.).

V prípade, že procesy riadenia rizík v prostredí prevádzkovateľa IS sú na to pripravené, je možné hodnotiť u niektorých existujúcich opatrení aj ich maturitu (vyspelosť). Toto hodnotenie je opodstatnené primárne pri organizačných a procesne orientovaných opatreniach. Pri špecifických technologických opatreniach sa hodnotí iba s nimi súvisiace procesné opatrenie.

4.7. Závažnosť rizík pre kvalitatívne a semikvalitatívne metódy

Ohodnotenie závažnosti rizík je vyjadrené stupňom podľa nasledovných sémantických významov:

Úroveň závažnosti	Slovný opis závažnosti
Veľmi vysoké	riziko bezprostredne a závažne ohrozuje primárne aktíva, bezpečnosť organizácie, resp. kritického procesu, alebo systému (typicky prekročenie stanoveného limitu tolerancie rizika, katastrofálna finančná strata alebo škoda na majetku, následky na zdravie a život, na životné prostredie, atď.)
Vysoké	riziko závažne ohrozuje primárne aktíva, bezpečnosť organizácie resp. kritického procesu, alebo systému
Stredné	riziko potenciálne ohrozuje primárne aktíva, bezpečnosť organizácie resp. kritického procesu, alebo systému
Nízke	riziko neohrozuje primárne aktíva, ohrozuje výkon niektorých podporných procesov, kritické procesy, alebo systémy však nie sú rizikom ohrozené
Veľmi nízke	riziko neohrozuje primárne aktíva, výkon procesov a prevádzka systémov nie sú rizikom ohrozené

Nasledujúcimi fázami v procese riadenia rizík je určenie metódy ošetrenia rizika a následne komunikácia rizika.

5. Kvalitatívna analýza rizík

5.1. Všeobecný popis fáz kvalitatívnej analýzy rizík

Metodika kvalitatívnej analýzy rizík popísaná v tomto dokumente pozostáva z nasledujúcich fáz:

1. Identifikácia scenárov rizík
2. Vyhodnotenie výsledného rizika pre identifikované scenáre rizík
   a) určenie pravdepodobnosti naplnenia scenárov rizík,
   b) ohodnotenie následkov,
   c) určenie úrovne závažnosti výsledných rizík.

5.2. Identifikácia scenárov rizík

Scenáre rizík predstavujú špecifické situácie realizácie rizík v kontexte vybraných aktív, pričom môžu byť kombináciou viacerých hrozieb a zraniteľností ústiacich do rôznych následkov.[8] Inak povedané – ide o sled alebo kombináciu udalostí vedúcich od počiatočnej príčiny k nežiaducemu následku.[9]

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. V rámci popisu scenárov rizík majú byť popísané okolnosti realizácie daného scenára rizika, príp. uvedené aj konkrétne zistené nedostatky.

Praktický výkon a mieru detailu dokumentácie tejto fázy je v praxi vhodné prispôsobiť veľkosti organizácie, zložitosti jej procesov a informačných systémov a celkovému významu kybernetickej a informačnej bezpečnosti pre správny chod organizácie. Detail je tiež závislý od pohľadu ktorý sa použil pre usporiadanie hierarchie informačných aktív (viď 4.1)

5.3. Posúdenie rizika kvalitatívnou metódou

Výsledné riziko v identifikovanom scenári sa určuje ako **prienik príslušnej hodnoty pravdepodobnosti naplnenia scenára rizika a hodnoty úrovne následkov, 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 následku. Popis existujúcich opatrení musí byť súčasťou popisu analyzovaného rizika, príp. oblasti bezpečnosti, ku ktorej riziko patrí.

5.3.1. Určenie pravdepodobnosti naplnenia scenára rizika

Pri určovaní pravdepodobnosti naplnenia scenára rizika sa vychádza z jeho predpokladaného naplnenia v stanovenom časovom horizonte (napr. dva roky). V analýze rizík je táto pravdepodobnosť vyjadrená nasledujúcim rozsahom:

Pravdepodobnosť	Pravdepodobnosť popisne
Veľmi vysoká	je takmer isté, že v stanovenom čase nastane naplnenie scenára rizika, pretože existujú súvisiace zneužiteľné zraniteľnosti a nie sú zavedené žiadne bezpečnostné opatrenia na ochranu

[8] NIST Special Publication 800-39 Managing Information Security Risk, NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments

[9] STN ISO/IEC 27005:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia – Usmernenie k riadeniu rizík informačnej bezpečnosti

Vysoká	je pravdepodobné, že v stanovenom čase nastane naplnenie scenára rizika, pretože existujú súvisiace zneužiteľné zraniteľnosti a zavedené bezpečnostné opatrenia sú neefektívne alebo zastarané
Stredná	je potenciálne možné, že v stanovenom čase nastane naplnenie scenára rizika, pretože existujú zneužiteľné zraniteľnosti a zavedené bezpečnostné opatrenia by mohli byť vylepšené
Nízka	je nepravdepodobné, že v stanovenom čase nastane naplnenie scenára rizika, pretože súvisiace zraniteľnosti boli pokryté vhodnými bezpečnostnými opatreniami
Veľmi nízka	je vysoko nepravdepodobné, že by v stanovenom čase malo nastať naplnenie scenára rizika, pretože súvisiace zraniteľnosti boli pokryté efektívnymi bezpečnostnými opatreniami

5.3.2. Ohodnotenie následkov pri naplnení scenára rizika

Pri ohodnocovaní závažnosti následkov v rámci jednotlivých scenárov rizík sú následky klasifikované podľa úrovne ich závažnosti. Úroveň závažnosti následkov je vyjadrená podľa nasledovných významov:

Následok	Následok popisne
Katastrofický	zásadné ohrozenie výkonu a funkčnosti primárnych procesov, kľúčových aktív; v extrémnom prípade ohrozenie bezpečnosti až existencie kritických aktív vo veľkom rozsahu, resp. celej organizácie
Závažný	prerušenie výkonu určitej konkrétnej služby alebo spôsobenie preukázateľného narušenia bezpečnosti, výdavky na riešenie bezpečnostného incidentu, zvýšené nároky na použitie mimoriadnych personálnych a finančných zdrojov na odstránenie dôsledkov, resp. prerušenie stredne významných činností
Stredný	následok neakceptovateľného charakteru, ktorý nie je zvládnuteľný v rámci plnenia bežných pracovných povinností a generuje personálne a finančné nároky (napr. zapojenie externých špecialistov a zdroje nad rámec bežného rozpočtu)
Malý	následok neakceptovateľného charakteru, ktorý však môže byť zvládnutý v rámci plnenia bežných pracovných povinností s minimálnymi personálnymi a finančnými nárokmi
Zanedbateľný	následok akceptovateľného charakteru, ktorý môže byť zvládnutý v rámci plnenia bežných pracovných povinností bez potreby dodatočných zdrojov na odstránenie dôsledkov

5.3.3. Určenie úrovne výsledného rizika

Výsledné riziko sa určuje ako kombinácia pravdepodobnosti naplnenia scenára rizika a závažnosti „najhoršieho“ následku. Pri určovaní výsledného rizika sa vychádza z nasledujúcej tabuľky:

Matica určenia úrovne výsledného rizika kvalitatívnou metódou:

Pravdepodobnosť	**Následok**				
	Zanedbateľný	**Malý**	**Stredný**	**Závažný**	**Katastrofický**
Veľmi vysoká	Stredné	Stredné	Vysoké	Veľmi vysoké	Veľmi vysoké
Vysoká	Nízke	Stredné	Vysoké	Vysoké	Veľmi vysoké

Stredná	Nízke	Stredné	Stredné	Vysoké	Vysoké
Nízka	Veľmi nízke	Nízke	Stredné	Stredné	Stredné
Veľmi nízka	Veľmi nízke	Veľmi nízke	Nízke	Nízke	Stredné

Klasifikácia závažnosti rizika pri použití kvalitatívnej metódy vyplýva priamo z matice pre určenie úrovne výsledného rizika a významovo je vysvetlená v kap. 4.7.

6. Semikvantitatívna (zmiešaná) analýza rizík

6.1. Všeobecný popis fáz zmiešanej analýzy rizík

Metodika semikvantitatívnej analýzy rizík popísaná v tomto dokumente pozostáva z nasledujúcich fáz:

1. Stanovenie jednotného indexu rizika
2. Identifikácia relevantných zraniteľností a hrozieb
3. Posúdenie rizika
   a) určenie hodnoty pravdepodobnosti jednotlivých hrozieb v súvislosti s daným aktívom,
   b) určenie hodnoty následku jednotlivých hrozieb v súvislosti s daným aktívom,
   c) výpočet úrovne závažnosti výsledných rizík.

6.2. Stanovenie jednotného indexu rizika

Pre stanovenie úrovne závažnosti rizika v metodike riadenia rizika je možné použiť napr. nasledovný index:

Úroveň závažnosti	Dolná hranica	Horná hranica
Veľmi vysoké	80	100
Vysoké	45	79
Stredné	20	44
Nízke	10	19
Veľmi nízke	1	9

Detailný výpočet úrovne závažnosti rizika je uvedený v časti 6.4.3.

Jednotný index úrovní rizika musí byť následne použitý a konsolidovaný vo všetkých dokumentoch a výstupoch hodnotenia rizika.

Definícia úrovní rizika je závislá od odvetvia a rizikového apetítu organizácie a tolerancie rizika v organizácii. Stanovenie úrovne rizika záleží na rozhodnutí vlastníkov rizika.

6.3. Identifikácia relevantných zraniteľností a hrozieb

V zmiešanej metóde sa uplatňuje prístup orientovaný na aktíva a následky (Asset-Impact oriented).

V prvom kroku je nutné identifikovať potenciálne dotknuté aktíva, následne identifikovať potenciálne zraniteľnosti týchto aktív a na základe týchto údajov rozhodnúť o hrozbách z referenčného katalógu hrozieb, ktoré môžu byť relevantné pre tieto aktíva v kontexte identifikovaných zraniteľností.

Do výsledného posúdenia budú zahrnuté len tieto identifikované hrozby. Pre každú z týchto hrozieb sa musí jednotlivo určiť hodnota pravdepodobnosti a určiť hodnota následku rizika podľa postupov v časti 6.4.

6.4. Posúdenie rizika zmiešanou metódou

V semikvantitatívnej analýze rizika sa pre definovanie rizikových faktorov používa numerický rozsah hodnôt so slovne vyjadreným kontextom. Hodnoty pravdepodobnosti a následku sú odvodené z rozsahu číselnej stupnice s priradením príslušného stupňa jedinečného významu.

6.4.1. Určenie hodnoty pravdepodobnosti

Pravdepodobnosť, že potenciálna zraniteľnosť môže byť zneužitá zo strany zdroja hrozby, môže byť popísaná ako veľmi vysoká, vysoká, stredná, nízka alebo veľmi nízka. Podrobnejšie rozdelenie a popis je v nasledujúcej tabuľke:

Pravdepodobnosť	%	Frekvencia slovne	Pravdepodobnosť popisne	Hod-nota
Veľmi 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 zraniteľnosť bola už mnohokrát zneužitá.	**1**
Vysoká	61 – 80	Často	Zdroj hrozby je motivovaný a technicky zdatný; uplatnené opatrenia čiastočne bránia úspešnému zneužitiu zraniteľností. Existuje skúsenosť z minulosti, že daná zraniteľnosť bola už niekoľkokrát zneužitá.	**0,8**
Stredná	41 – 60	Niekedy	Zdroj hrozby je čiastočne motivovaný a technicky zdatný; uplatnené opatrenia pomerne úspešne bránia úspešnému zneužitiu zraniteľností. Existuje skúsenosť z minulosti, že daná zraniteľnosť bola zneužitá.	**0,6**
Nízka	21 – 40	Málokedy	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľností. Z minulosti existuje ojedinelá skúsenosť zneužitia danej zraniteľnosti.	**0,4**
Veľmi nízka	0 – 20	Skoro nikdy	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľností. Neexistuje historická skúsenosť so zneužitím danej zraniteľnosti.	**0,2**

6.4.2. Určenie hodnoty následku

Hodnoty následku je nevyhnutné určovať pre každú organizáciu individuálne. Nasledovná tabuľka určuje príklad hodnôt pre semikvantitatívne riadenie rizík.

Opis následku	Finančný následok (príklad)	Prevádzkový následok	Následok na súlad	Reputačný následok	Hod-nota
Katastrofický	1 500 001 – 15 000 000 €	Organizácia, všetci klienti	Pozastavenie časti služieb / ukončenie činnosti	Intenzívna nepriaznivá publicita na národnej, alebo medzinárodnej úrovni	**100**
Závažný	150 001 – 1 500 000 €	Organizácia, značná časť klientov	Začatie správneho konania smerujúce k uloženiu pokuty alebo iný peňažný dopad (pokuta zo zmluvy)	Nepriaznivá publicita, prípadne na národnej úrovni	**80**
Stredný	15 001 – 150 000 €	Organizácia, malá časť klientov	Začatie správneho konania smerujúce k opatreniu na nápravu	Závažné prekážky v externej komunikácii	**60**
Malý	1501 – 15 000 €	Interne, viacero útvarov	Zlyhanie kritických procesov	Prekážky v komunikácii v rámci organizácie	**40**
Zanedbateľný	1 – 1500 €	Interne, jeden útvar	Zlyhanie interného procesu	Určité prekážky v komunikácii v rámci organizácie	**20**

6.4.3. Výpočet úrovne závažnosti rizík

Úroveň závažnosti rizika [R] je vyhodnocovaná ako násobok stanovenej pravdepodobnosti rizika [P] a stanoveného následku rizika [D]. Všeobecne je funkcia pre výpočet rizika uvádzaná ako:

$$R = P \times D$$

Výsledné hodnoty množiny je následne možné zaradiť v dvojrozmernej matici:

Pravdepodobnosť	**Následok**				
	Zanedbateľný (20)	**Malý (40)**	**Stredný (60)**	**Závažný (80)**	**Katastrofický (100)**
Veľmi vysoká (1)	20	40	60	80	100
Vysoká (0,8)	16	32	48	64	80
Stredná (0,6)	12	24	36	48	60
Nízka (0,4)	8	16	24	32	40

Veľmi nízka (0,2)	4	8	12	16	20

Klasifikácia úrovne závažnosti rizík je nasledujúca:

Úroveň rizika číselne	Úroveň závažnosti rizika slovne
od 80 do 100	Veľmi vysoké
od 45 do 79	Vysoké
od 20 do 44	Stredné
od 10 do 19	Nízke
od 1 do 9	Veľmi nízke

Pre jednotlivé aktíva sú hodnotené len tie položky z katalógu hrozieb, ktoré sú relevantné pre konkrétne aktívum. Pre každú z relevantných hrozieb pre príslušné aktívum sa určí úroveň závažnosti rizika. Výsledná hodnota úrovne závažnosti rizika v kontexte informačného aktíva [R] bude potom súčtom rizika každej z relevantných hrozieb z referenčného katalógu hrozieb, t. j.:

$$R = \sum R_1 \dots R_n$$

Jednotlivé hrozby môžu byť (resp. typicky aj sú) zreťazené. Tieto je možné vyjadriť prostredníctvom scenára rizika ako opisu škodlivej udalosti. Riziková expozícia dotknutých informačných aktív v scenári bude potom priemerom rizika pre hrozby, ktoré sú súčasťou scenára, podľa podobného vzorca, t. j.:

$$\bar{R}_s = \frac{1}{n} \sum_{i=1}^{n} R_i$$

Riziková expozícia informačného aktíva sa teda vypočítava ako aritmetický priemer tak, že súčet rizík relevantných hrozieb vstupujúcich do scenára sa vydelí počtom relevantných hrozieb vstupujúcich do scenára.

Je potrebné uviesť, že v prístupe orientovanom na zraniteľnosti môže byť identifikácia hrozieb založená na identifikácii aktív a ich vlastníkov a identifikácii **zraniteľností** [V] potenciálne pôsobiacich na tieto aktíva. Funkcia pre výpočet rizika je potom uvádzaná spolu s hodnotou zraniteľnosti, tiež ako:

$$R = P \times D \times V$$

7. Kvantitatívna analýza rizík

7.1. Všeobecný popis fáz kvantitatívnej analýzy rizík

Metodika kvantitatívnej analýzy rizík popísaná v tomto dokumente pozostáva z nasledujúcich fáz:

1. Identifikácia scenárov rizík
2. Stanovenie modelu rizika a nákladových faktorov pro daný scenár
3. Identifikácia relevantných zraniteľností a hrozieb
4. Posúdenie rizika
   a) určenie hodnoty pravdepodobnosti jednotlivých hrozieb v súvislosti s daným aktívom,
   b) určenie hodnoty následku jednotlivých hrozieb v súvislosti s daným aktívom,
   c) výpočet úrovne závažnosti výsledných rizík.

7.2. Identifikácia scenárov rizík

Scenáre rizík predstavujú špecifické situácie realizácie rizík v kontexte organizácie a vybraných aktív (vrátane kľúčových obchodných procesov), pričom jeden scenár môže viesť k viacerým rôznym následkom. Ide o zjednodušený sled alebo kombináciu udalostí, ktorý vždy obsahuje spúšťač (t. j. počiatočnú udalosť, ktorá spustí celý sled, typicky spojenú s prvotnou príčinou) a všetky relevantné a zároveň nákladovo významné typy nežiaducich následkov (napr. výpadok kľúčového obchodného procesu, sprenevera finančných prostriedkov, náklady a pokuty spojené so stratou dôvernosti citlivých údajov).

Pred samotným vykonaním analýzy rizík je potrebné identifikovať všetky podkladové materiály na popis scenárov rizík, napríklad odhadovanú alebo nameranú frekvenciu výskytu daného konkrétneho scenára v zvažovanej populácii (referenčnej skupine/triede) a odhadovanú (orientačnú) materiálnu závažnosť naplnenia daného scenára v organizácii pri zohľadnení existujúcich opatrení, okolností realizácie daného scenára rizika, prípadne aj konkrétne zistené nedostatky, ktoré by oproti referenčnej triede zvýšili frekvenciu alebo zhoršili následky.

Praktické vykonanie a mieru detailu dokumentácie tejto fázy je potrebné v praxi prispôsobiť typu, geografickému dosahu a veľkosti organizácie, požiadavkám sektorovej regulácie a celkovému významu kybernetickej a informačnej bezpečnosti pre správne fungovanie organizácie.

7.3. Posúdenie rizika kvantitatívnou metódou

Dielčia zložka rizika v identifikovanom scenári sa určuje pre každý identifikovaný (nákladovo významný) typ následku ako matematický súčin príslušnej hodnoty anualizovanej pravdepodobnosti (prípadne anualizovanej početnosti) naplnenia scenára rizika a štatistickej krivky typu hustota pravdepodobnosti (pravdepodobnostná distribučná funkcia – PDF) možnej veľkosti následkov daného typu v peňažných jednotkách. Výsledné riziko v identifikovanom scenári sa určuje ako matematický súčet (agregácia) dielčích zložiek rizika (štatistických kriviek PDF), pričom výsledkom je celková štatistická krivka (PDF).

Na účely jednotného reportovania sa z výslednej krivky vypočítajú kľúčové charakteristiky, typicky očakávaná (stredná) hodnota (EV) a hodnoty pre percentily P50, P95 a P99, prípadne parametre kumulatívnej distribučnej funkcie (CDF), ktoré určujú hodnotu ohrozenú rizikom, typicky VaR 90, VaR 95 a VaR 99.

Pri samotnom výpočte výsledného rizika sa zohľadňuje aj úroveň existujúcich opatrení, ktoré môžu ovplyvniť hodnoty pravdepodobnosti (frekvencie) alebo tvar štatistickej krivky (PDF) pre daný typ

následku. Popis existujúcich opatrení musí byť súčasťou popisu analyzovaného rizika, prípadne oblasti bezpečnosti, ku ktorej riziko patrí.

7.3.1. Určenie pravdepodobnosti naplnenia scenára rizika

Pri určovaní pravdepodobnosti naplnenia scenára rizika sa vychádza z jeho predpokladaného výskytu v stanovenom časovom horizonte (typicky jeden rok, teda anualizovane). Pri odhade pravdepodobnosti sa zohľadňuje vnútorná situácia organizácie (historické údaje o takmer-nehodách a incidentoch za uplynulé relevantné obdobia) a vonkajšia situácia vo zvolenej referenčnej triede (výskyt incidentov za rovnaké obdobia). Vykonáva sa tzv. kalibrovaný expertný odhad (bodový alebo intervalový) frekvencie (napr. raz za päť rokov – typ 1-in-5) alebo anualizovanej pravdepodobnosti (napr. P = 20 %).

Alternatívne je možné expertný (subjektívny) odhad zahrnúť vo forme tzv. prioru do formálneho (matematického) spracovania spolu s objektívnymi údajmi (historickými dátami o vnútornej a vonkajšej situácii) využitím Bayesovských štatistických metód. V prípade dostatočného množstva historických údajov nie je potrebné expertný odhad zohľadňovať – na určenie pravdepodobnosti sa použijú bežné štatistické metódy (typicky založené na počte príležitostí k zlyhaniu za rok, pravdepodobnosti zlyhania a pravdepodobnosti včasnej detekcie takéhoto zlyhania).

7.4. Ohodnotenie následkov pri naplnení scenára rizika

Pri hodnotení závažnosti následkov v rámci jednotlivých scenárov rizík sú nákladovo významné následky rozdelené podľa typu. Pre každý typ je potrebné určiť nákladový faktor (cost factor, CF) ako merateľnú veličinu ovplyvňujúcu výšku straty v peňažných jednotkách (napr. minúta výpadku kľúčového obchodného procesu alebo hodina neproduktivity zamestnanca alebo počet uniknutých citlivých záznamov/údajov), ako aj mechanizmus a parametre prevodu na peňažné jednotky (hodinová strata, hodinová mzda, jednotkové náklady za uniknutý záznam pre daný rozsah úniku údajov).

Každý identifikovaný (nákladovo významný) typ následku tvorí dielčiu zložku rizika s príslušným štatistickým rozložením následkov v danej merateľnej veličine (napr. minúty, počty záznamov). Pre tieto veličiny sa vykonáva tzv. kalibrovaný expertný odhad (vždy intervalový) na príslušnej úrovni spoľahlivosti (kredibility). Pri odhade sa zohľadňuje vnútorná situácia organizácie (schopnosť zvládnuť výpadok/nedostupnosť, množstvo citlivých záznamov, limity na okamžitý prevod peňazí) a vonkajšia situácia vo zvolenej referenčnej triede (následky hlásených incidentov, stredné hodnoty pre dané typy škôd).

Intervalové (viacbodové) odhady spolu s prevodnými parametrami a výberom vhodného štatistického rozdelenia (napr. log-normálne rozdelenie) slúžia na konštrukciu štatistickej krivky možných následkov (pravdepodobnostnej distribučnej funkcie – PDF) daného typu (dielčej zložky rizika) v peňažných jednotkách.

7.4.1. Určenie úrovne výsledného rizika

Dielčia zložka rizika v identifikovanom scenári sa určuje pre každý identifikovaný (nákladovo významný) typ následku ako matematický súčin príslušnej hodnoty anualizovanej pravdepodobnosti (prípadne anualizovanej početnosti) naplnenia scenára rizika a štatistickej krivky (pravdepodobnostnej distribučnej funkcie – PDF) možnej veľkosti následkov daného typu v peňažných jednotkách.

Výsledné riziko v identifikovanom scenári sa určuje ako matematický súčet (agregácia) dielčích zložiek rizika (štatistických kriviek PDF), pričom výsledkom je celková štatistická krivka (PDF).

Na určenie tzv. materiality rizika a na jednotné reportovanie rizík sa z výslednej krivky vypočítajú kľúčové štatistické charakteristiky. Typicky ide o očakávanú (strednú) hodnotu (EV) a hodnoty

pre percentily P50, P95 a P99, prípadne parametre kumulatívnej distribučnej funkcie (CDF), ktoré určujú hodnotu ohrozenú rizikom – typicky VaR 90, VaR 95 a VaR 99.

Detaily sa líšia v závislosti od konkrétnej organizácie, regulačného rámca, regionálnych požiadaviek a sektorových osvedčených postupov.

Klasifikácia úrovne závažnosti rizík je nasledujúca:

- Materiálne riziko – jedna alebo viacero kľúčových štatistických charakteristík prekročila definovaný prah materiality (napr. očakávaná hodnota rizika EV je vyššia než stanovená hodnota ekonomického indikátora, napr. vyššia než 5 % trhovej hodnoty organizácie). V tomto prípade bude výsledná krivka rizika použitá na stanovenie špeciálnych cieľov (KRO) a peciálnych indikátorov (KRI) pre tvorbu následného plánu zvládania rizík.
- Nemateriálne riziko – žiadna z kľúčových štatistických charakteristík neprekročila definovaný prah materiality (napr. očakávaná hodnota rizika EV je nižšia než stanovená hodnota ekonomického indikátora, napr. nižšia než 5 % trhovej hodnoty organizácie). V tomto prípade bude výsledná krivka rizika použitá v agregácii (t. j. na určenie celkovej expozície organizácie voči kybernetickým rizikám) na definovanie všeobecnej stratégie zvládania rizík (výber všeobecných/plošných opatrení, nastavenie limitov poistenia a finančných rezerv).

8. Ošetrovanie rizika

8.1. Metódy ošetrenia rizika

Pri výbere a prijímaní opatrení sa zohľadňujú nasledovné základné prístupy k riziku:

8.1.1. Zníženie rizika

Zníženie rizika je najčastejšou metódou ošetrenia rizika. Uplatnený je výber vhodných opatrení tak, aby riziko bolo znížené až na úroveň zvyškového rizika, ktoré môže byť následne prehodnotené ako akceptovateľné.

Zníženie rizika je možné dosiahnuť pomocou vhodných opatrení na zníženie následkov rizika alebo na zníženie pravdepodobnosti realizácie rizika (napr. pri riziku útoku na IS alebo infiltrácie zo siete internet sa nasadia adekvátne nakonfigurované firewally a ďalšie bezpečnostné nástroje).

8.1.2. Vyhnutie sa riziku

Keď je identifikované riziko považované za príliš vysoké, alebo náklady na implementáciu ošetrenia rizika presahujú prínosy, rozhodnutím môže byť aj úplné vyhnutie sa riziku, a to nevykonaním plánovanej alebo existujúcej aktivity alebo súboru aktivít, resp. zmenou podmienok, podľa ktorých bude činnosť vykonávaná.

Najčastejším spôsobom vyhnutia sa riziku je rozhodnutie zmeniť prostredie, v ktorom sa riziko vyskytuje tak, aby toto riziko neprichádzalo do úvahy (napr. v prípade ohrozenia dôvernosti údajov pri ich prenose nedôveryhodným komunikačným kanálom sa použije iný komunikačný kanál),

8.1.3. Presun rizika

Presun rizika je metóda ošetrenia rizika, pri ktorej bude určitá časť následkov rizika zdieľaná s externými subjektmi. Typickým presunom rizika je poistenie, alebo výber zmluvného partnera, ktorého úlohou bude monitorovať proces a prijať okamžité opatrenia na zastavenie hrozby skôr, ako vznikne škoda. (napr. pri zvýšenom riziku požiaru sa organizácia poistí proti stratám spôsobeným požiarom).

8.1.4. Zachovanie rizika

Ak úroveň rizika spĺňa kritériá na akceptáciu rizika, nie je potrebné implementovať opatrenia a riziko môže zostať zachované v pôvodne ohodnotenej úrovni.

8.2. Návrh bezpečnostných opatrení

V zmysle všeobecných zásad tejto metodiky majú byť riziká ošetrované v poradí od najvyšších po najnižšie. Bezpečnostné opatrenia musia byť preto prijímané v závislosti na stanovenej úrovni rizika.

Návrh opatrení v závislosti na stanovenej úrovni závažnosti rizika pre kvalitatívne a semikvantitatívne riadenie rizík.

Úroveň závažnosti rizika	Opatrenia
Veľmi 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 opatrení.

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.
Stredné riziko	Rozšírené, príp. dodatočné bezpečnostné opatrenia sú potrebné a mali by byť prijaté v dobe, ktorú určí vlastník rizika. Výkon kľúčových procesov organizácie ani prevádzka systému sa nepovažujú za akútne ohrozené.
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.
Veľmi nízke riziko	Nie je nutné prijať dodatočné ani rozšírené bezpečnostné opatrenia. Riziko je možné akceptovať ako prijateľné.

Štruktúra opatrení podľa tejto metodiky je založená na štruktúre podľa Vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach.

Návrh bezpečnostných opatrení vychádza z nasledovných princípov:

- pri návrhu opatrení sa vychádza z hodnoty a charakteru výsledného rizika určeného podľa stanovenej metodiky,
- pre každé výsledné riziko, ktoré nie je akceptovateľné, je popísaný spôsob jeho ošetrenia pomocou navrhovaných bezpečnostných opatrení,
- opatrenia sú navrhované v kontexte identifikovaných hrozieb,
- cieľom je navrhnúť systém bezpečnostných opatrení takým spôsobom, aby po ich implementácii boli všetky riziká znížené na úroveň zodpovedajúcu akceptovateľným rizikám.

Typy opatrení v kontexte životného cyklu informačného aktíva:

- **Existujúce** opatrenia (z angl. Existing controls) – opatrenia inherentne zabudované už v čase návrhu resp. implementácie systému
- **Rozšírené** (tiež „vylepšené“) opatrenia (z angl. Enhanced controls) – aplikované na implementovaný systém s cieľom ošetrenia rizika identifikovaného už v rámci bežnej prevádzky systému; typicky ich navrhuje manažér KB
- **Dodatočné** opatrenia (z angl. Additional, Complementary controls) - odporúča ich typicky audítor v správe auditu s cieľom ošetrenia rizika identifikovaného v rámci výkonu auditu kybernetickej bezpečnosti

Z hľadiska realizácie opatrení na zníženie rizika je potrebné opatrenia rozdeliť na:

- **Operatívne** – t. j. opatrenia, ktorých implementácia je z časového a finančného hľadiska nenáročná, ale ktorých účinok prináša bezprostredný efekt na zníženie rizika,
- **Systémové** - t. j. organizačné a rozsiahlejšie technické opatrenia s dlhodobým účinkom na znižovanie rizika.

Postupnosť, akou budú navrhované opatrenia realizované, tzv. implementačný plán, je rozpracovaná v rámci bezpečnostnej stratégie, resp. bezpečnostného projektu. Tento program závisí od viacerých faktorov, ktoré je potrebné pri jeho návrhu zohľadniť. K takýmto faktorom prináležia:

- priority vyplývajúce z ohodnotenia rizík,
- výška nákladov potrebných na realizáciu opatrení,

- pripravenosť a spôsobilosť organizácie na realizáciu opatrení (technická, organizačná, finančná),
- podpora manažmentu organizácie na realizáciu opatrení.

8.2.1. Operatívne opatrenia

Cieľom operatívnych opatrení je uplatnenie takých zmien procesov a technológií, ktoré budú viesť k urýchlenému zníženiu identifikovaného rizika s čo najnižšími nákladmi a najvyšším účinkom.

Za rozhodnutie o prijatí operatívnych opatrení je zodpovedný manažér kybernetickej bezpečnosti, s následnou povinnosťou potvrdenia prijatých opatrení zo strany vedenia.

8.2.2. Systémové opatrenia

Cieľom systémových opatrení je zvoliť optimálnu hranicu medzi účinnosťou bezpečnostných mechanizmov a požiadavkami, ktoré sú kladené na prevádzku aktív. Výsledkom systémových opatrení musí byť proaktívny prístup k riadeniu rizika, ktoré umožní:

- identifikovať riziko v počiatočnom štádiu pôsobenia príslušnej hrozby a existencie príslušnej zraniteľnosti,
- monitorovať riziko počas pôsobenia príslušnej hrozby a existencie príslušnej zraniteľnosti,
- eliminovať následky rizika na funkčnosť IS,
- zdokumentovať priebeh rizika.

Navrhované systémové opatrenia musia byť predložené na najbližšom rokovaní vedenia na schválenie a následnú realizáciu.

9. Akceptácia zvyškového rizika

9.1. Zvyškové riziko

Akceptovateľné zvyškové riziko je riziko, ktorého hodnota po komplexnom ošetrení rizík implementáciou pôvodných, dodatočných a rozšírených opatrení je taká nízka, že je pre organizáciu prijateľné a nie je nutné uplatniť ďalšie opatrenia na jeho zníženie.

Výsledné riziko môže byť v rámci analýzy rizík označené ako akceptovateľné len za predpokladu splnenia nasledovných podmienok:

- pravdepodobnosť realizácie rizika je príliš nízka,
- straty spôsobené realizáciou rizika sú nepatrné,
- realizácia rizika výrazne nenaruší stanovenú / očakávanú úroveň bezpečnosti,
- opatrenia minimalizujúce pravdepodobnosť jeho realizácie sú nákladnejšie ako prípadné straty,
- opatrenia minimalizujúce pravdepodobnosť jeho realizácie výrazne prevyšujú štandardnú úroveň bezpečnosti v prostredí nasadenia,
- akceptácia nepovedie k porušeniu právnych, regulačných alebo zmluvných požiadaviek,
- pri presune rizika na iný subjekt.

Referenčná hodnota zvyškového rizika by mala byť stanovená na takej úrovni, aby riziko bolo možné zanedbať. Keďže zvyškové riziko musí byť zanedbateľné, vylučuje to možnosť označiť vysoké riziko za zvyškové.

9.2. Kritériá akceptácie zvyškového rizika

Návrhy možných prístupov (resp. hodnotiacich kritérií) pre prijatie zvyškového rizika:

- vyjadrenie kritérií prijatia rizika ako pomeru odhadnutého zisku (alebo iného podnikateľského prospechu) k odhadnutému riziku
- stanovenie rôznych tried rizík (napr. rizík, ktoré by mohli viesť k nesúladu s právnymi a regulačnými požiadavkami, resp. rizík stanovených zmluvnými požiadavkami)
- požiadavky na budúce dodatočné ošetrenie (napr. riziko môže byť prijaté, ak existuje schválenie a záväzok zníženia rizika na prijateľnú úroveň v stanovenom časovom období)

Kritéria prijatia rizík sa môžu líšiť v závislosti na tom, ako dlho sa očakáva, že riziko bude existovať, napr. riziko môže byť spojené s dočasnou, alebo krátkodobou aktivitou. Kritéria pre prijatia rizika by mali byť stanovené so zreteľom na:

- Obchodné požiadavky
- Právne a regulačné aspekty
- Bežnú prevádzku
- Technológie
- Financie
- Sociálne a humanitárne faktory

9.3. Proces akceptácie rizika

Akceptácia zvyškového rizika je proces, v ktorom štatutárne vedenie organizácie, alebo štatutárnym zástupcom poverený organizačný útvar formálne odsúhlasí eskalované zvyškové riziko.

Pre štatutárne vedenie organizácie ako vlastníkov rizika je odporúčané predložiť návrh na akceptáciu rizika vo formáte, ktorý obsahuje všetky informácie potrebné k rozhodnutiu o akceptácii.

Vzor formulára pre akceptáciu rizika je v prílohe č.1. Všetky akceptované riziká musia byť prehodnocované minimálne raz ročne a to až do doby, pokiaľ riziko neprestane byť relevantné, alebo sa nepristúpi k inému spôsobu ošetrenia identifikovaného a trvajúceho rizika.

10. Komunikácia rizika

Komunikácia rizika je kontinuálny a iteratívny proces, ktorý organizácia vykonáva s cieľom poskytovať, zdieľať alebo získavať informácie a nadviazať dialóg so zainteresovanými stranami o riadení rizika.

Organizácia by mala vytvoriť mechanizmy internej komunikácie a reportingu s cieľom podporovať a prijať zodpovednosť za riadenie rizika. Tieto mechanizmy by mali zabezpečiť, aby:

- kľúčové súčasti rámca riadenia rizík a všetky následné úpravy boli primerane komunikované
- existoval vhodný interný reporting o rámci riadenia rizík, jeho účinnosti a výsledkoch
- relevantné informácie odvodené z riadenia rizík boli včas k dispozícii na príslušných úrovniach riadenia
- existovali procesy konzultácie rizika so zainteresovanými stranami

Tieto mechanizmy by podľa potreby mali zahŕňať postupy na konsolidáciu informácií o rizikách z rôznych zdrojov.

10.1. Správa o riziku

Identifikácia a ohodnotenie všetkých rizík uvažovaných v rámci analýzy rizík (a v nej identifikovaných scenárov) by mali byť uvádzané a sledované v Zozname rizík.

V závislosti od veľkosti a zložitosti organizácie a jej informačných systémov môže byť zoznam rizík vedený v rôznom detaile. Pre menšie subjekty môže byť zoznam rizík vedený napríklad vo forme jednoduchého zoznamu, napr. v dokumente MS Excel. Pre väčšie organizácie a komplexné informačné systémy môžu byť riziká a scenáre rizík evidované a spravované pomocou špecializovaných softvérových nástrojov a popísané v správach o riziku.

Vo vzťahu k informačným technológiám verejnej správy je veľkosť a zložitosť organizácie vymedzená kategóriami minimálnych bezpečnostných opatrení v osobitnom predpise.[10]

Vzor správy o riziku je v prílohe č. 2.

[10] Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

11. Prílohy

11.1. Vzor návrhu na akceptáciu rizika

ID:	196, 171, 172, 173	Stav ošetrenia rizika:	Na akceptáciu
Riziko:	Nepodporované operačné systémy s kritickými zraniteľnosťami na serveroch vystavených do internetu		
Opis rizika:	Servery bežia na nepodporovanom systéme Windows 2000 Server. OS obsahuje niekoľko kritických chýb zabezpečenia: (MS05-051) Vzdialené spustenie kódu Microsoft COM+/MSDTC. V službe Microsoft Distributed Transaction Coordinator (MSDTC), ktorá je súčasťou systému Microsoft Windows, existuje chyba zabezpečenia. Microsoft nevydáva bezpečnostné opravy pre nepodporované produkty. Podpora bola ukončená v roku 2013.		
Pravdepodobnosť:	Stredná (0,8)	Úroveň rizika:	Stredné (40)
Dopad:	Stredný (50)	Použitá metóda ošetrenia rizika:	Znižovanie rizika
Postup ošetrenia rizika:	**Doterajšie úkony:** • Požiadali sme dodávateľa, aby aplikovali bezpečnostné opravy. Komunikácia nebola úspešná. Aplikácia opráv bez podpory a testovania bude predstavovať riziko nefunkčnosti aplikácií. **Ďalší postup:** • Upgrade operačných systémov		

11.2. Vzor správy o riziku

ID	***Názov rizika***		
Popis rizika	Popis scenára alebo udalosti, ktorá môže ohroziť bezpečnosť		
Dotknuté aktíva	Identifikácia aktív, na ktoré sa príslušný scenár rizika vzťahuje		
Relevantné hrozby	Identifikácia hrozieb, ktoré sa podieľajú na tomto scenári rizika		
Zraniteľnosti	Identifikácia zraniteľností, ktoré sa podieľajú na danom scenári rizika		
Následky	Identifikácia následkov, ktoré môžu nastať po realizácii hrozieb		
Existujúce opatrenia			
1. opatrenie 2. opatrenie 3. opatrenie			
Úroveň následkov	Hodnota následkov	**Pravdepodobnosť naplnenia**	Hodnota pravdepodobnosti naplnenia
Výsledné riziko	**Veľmi vysoké/Vysoké/Stredné/Nízke/Veľmi nízke**		
Navrhované opatrenia			
1. opatrenie			

2. opatrenie
3. opatrenie

11.3. Typy aktív

Typ aktíva	Názov	Popis
Primárne	Elektronické dáta v databázach	Údaje usporiadané v štruktúrovanej podobe, typicky uložené a spracované pomocou systému riadenia bázy dát.
Primárne	Elektronické dáta v súboroch	Súbory údajov uložené lokálne, na serveroch, alebo v cloude.
Primárne	Ostatné nehmotné aktíva	Nehmotné aktíva, ktoré zahŕňajú dobré meno organizácie, právne požiadavky a vzťahy, autorské práva, iné duševné vlastníctvo.
Primárne	Papierové dáta	Informácie zaznamenané v písomnej forme, na papierovom nosiči. Táto forma ukladania informácií je charakteristická svojou materiálnou podstatou, čo umožňuje uchovávanie dát bez potreby elektrickej energie alebo digitálnych zariadení.
Primárne	Proces	Štruktúrovaný súbor vzájomne súvisiacich alebo vzájomne sa ovplyvňujúcich činností, navrhnutých tak, aby transformovali vstupy na výstupy a aby bol týmito činnosťami dosiahnutý konkrétny cieľ.
Primárne	Služba	Nehmotný spôsob poskytnutia hodnoty, alebo iného prospešného výsledku používateľovi, ktorá napomáha dosiahnuť požadované výsledky.
Primárne	Služba IS	Služba pozostávajúca úplne alebo prevažne z prenosu, ukladania, získavania alebo spracúvania informácií prostredníctvom IS.
Podporné	Aplikačný softvér	Softvér, ktorý vykonáva špecifické úlohy pre koncového používateľa alebo pre inú aplikáciu.
Podporné	Cloudové služby	Digitálne služby, ktoré umožňujú správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných počítačových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach. (Počítačové zdroje zahŕňajú zdroje, ako sú siete, servery alebo iná infraštruktúra, operačné systémy, softvér, úložiská, aplikácie a služby).
Podporné	Hardware	Akékoľvek zariadenie IKT/ITVS, nevyhnutné na ukladanie dát a vykonávanie softvéru, ktoré je

		napájané elektrickou energiou, zvyčajne riadené pomocou firmware (BIOS).
Podporné	Kľúčový dodávateľ	Kritická externá entita, ktorá poskytuje tovary alebo služby, ktoré sú nevyhnutné pre IS.
Podporné	Komunikačný kanál	Prostriedok, prostredníctvom ktorého sú informácie prenášané z jedného počítačového zariadenia na druhé.
Podporné	Lokalita	Fyzické priestory alebo geografická lokalita, kde sa vykonávajú prevádzkové činnosti
Podporné	Mobilný telefón	Elektronické zariadenie vybavené operačným systémom, ktoré kombinuje funkcie osobného počítača s funkciami telefónu a umožňuje používateľovi uskutočňovať hlasové hovory, posielať správy a pristupovať k aplikáciám.
Podporné	Notebook, prenosná pracovná stanica	Prenosné výpočtové zariadenie schopné vykonávať úlohy a pristupovať k dátam prostredníctvom aplikácií.
Podporné	Operačný systém	Softvér, ktorý riadi počítačový fyzický, alebo virtuálny hardvér a softvérové zdroje a poskytuje spoločné služby pre počítačové programy.
Podporné	Organizácia	Entita, ktorá zahŕňa viacero používateľov, procesov a služieb, ktoré spolu pracujú na dosiahnutí spoločného cieľa.
Podporné	Ostatné hmotné aktíva	Hmotné aktíva, ktoré vlastní a používa organizácia, ale nezahŕňajú nehnuteľnosti ani ITVS.
Podporné	PC, neprenosná pracovná stanica	Výpočtové zariadenie konštrukčne navrhnuté na stacionárne umiestnenie, s ohľadom na maximálnu rozšíriteľnosť, schopné vykonávať úlohy a pristupovať k dátam prostredníctvom aplikácií.
Podporné	Personál	Jednotlivci zamestnaní v organizácii, ktorí vykonávajú procesy a ktorí prispievajú k tvorbe výstupov.
Podporné	Počítačová sieť	Technická infraštruktúra, ktorá spája viaceré počítače a zariadenia za účelom zdieľania dát, zdrojov a služieb. Sieť môže byť realizovaná prostredníctvom káblových alebo bezdrôtových technológií, a môže operovať v rôznych geografických rozsahoch.

Podporné	Používateľ	Jednotlivec alebo skupina, ktorá je v interakcii alebo má prospech zo služby alebo služieb; príklady používateľov zahŕňajú osobu alebo komunitu ľudí.
Podporné	Prenosné dátové médiá	Prenosné dátové médiá sú fyzické alebo elektronické zariadenia alebo média, ktoré umožňujú ukladanie, prenos a zdieľanie digitálnych dát medzi rôznymi počítačmi alebo systémami bez potreby priameho pripojenia cez internet alebo lokálnu sieť. Tieto médiá sú navrhnuté tak, aby boli ľahko prenosné a kompatibilné s viacerými zariadeniami.
Podporné	Virtualizačná platforma	Softvér alebo firmware, ktorý vytvára a spravuje virtuálne stroje poskytovaním abstrakcie hardvérových zdrojov (ako sú procesory, pamäť, úložisko a sieťové zariadenia) a rozdeľovaním týchto zdrojov medzi rôzne virtuálne stroje. Tento proces umožňuje viacerým operačným systémom a ich aplikáciám beh na jednej fyzickej platforme s izoláciou a nezávislosťou od seba.

[i] Expertné odhady sú tzv. kalibrované, t. j. majú známu mieru chybovosti.