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

Verzia	1.0
Dátum vydania	13. decembra 2021
Dátum účinnosti	1. januára 2022

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 dopadov 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 finančných a 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.

Návody a usmernenia tejto metodiky sú uplatniteľné aj pre povinné osoby podľa osobitného predpisu. [1]

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 okolností, ktoré potenciálne môžu narušiť bezpečnosť (t.j. zraniteľností, hrozieb, scenárov hrozieb 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**.

Pre štatistické účely a pre potreby oznamovania kybernetických bezpečnostných incidentov **Úrad stanoví jednotnú metriku**. Pokiaľ má prevádzkovateľ implementovaný proces riadenia rizík s vyššou úrovňou vyspelosti, rozdielny od tejto metodiky, navrhne spôsob mapovania hodnôt z používanej metriky na požadovanú jednotnú metriku.

Výsledkom analýzy rizík musí byť ohodnotený zoznam identifikovaných rizík a návrh bezpečnostných opatrení, ktoré slúžia na ošetrenie týchto rizík.

Preferovanou metódou ošetrovania rizika má byť redukcia rizika na akceptovateľnú úroveň. Riziká majú byť primárne ošetrované v poradí od najvyšších po najnižšie.

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

Odhad pravdepodobnosti zohľadňuje najpravdepodobnejšiu kombináciu hrozieb, ktorej je následne priradená slovná, alebo číselná hodnota pravdepodobnosti naplnenia, v rámci stanovenej metriky.

Odhad závažnosti potenciálnych dopadov zohľadňuje najhorší možný dopad hrozieb, ktorému je následne priradená slovná, alebo číselná hodnota závažnosti dopadu, v rámci stanovenej metriky.

Vyhodnotenie výsledného rizika je vyjadrené ako násobok odhadu pravdepodobnosti a odhadu závažnosti dopadov plynúcich z možného naplnenia hrozby, škodlivej udalosti, alebo kombinácie hrozieb, po zohľadnení existujúcich bezpečnostných opatrení.

[1] Zákon č. 95/2019 Z. z. informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 95/2019 Z. z.“)

Identifikované zraniteľnosti, hrozby, potenciálne škodlivé udalosti sú sumarizované do konkrétnych scenárov rizík, v kontexte príslušného informačného aktíva.

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 resp. zákona č. 95/2019 Z.z. informačných technológiách vo verejnej správe.

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. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- ISO/IEC 27000:2018 Informačné technológie – Bezpečnostné metódy – Systém riadenia informačnej bezpečnosti – Prehľad a slovník
- ISO/IEC 27005:2018 Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti
- ISO 31000:2018 Manažérstvo rizika – Návod
- NIST Special Publication 800-39 Managing Information Security Risk
- NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments

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].

1.5. Definície a kľúčové pojmy

Pojem	Skratka	Výklad
aktíva		hmotné, alebo nehmotné statky, ktoré pre organizáciu priamo, alebo nepriamo predstavuje predstavujú súčasnú, alebo potenciálnu hodnotu. (Aktívami sú všeobecne najmä: procesy, know-how, dáta, informácie, software, služby, objekty, technologické komponenty a priestory organizácie).
analýza rizík		proces na pochopenie pôvodu rizík a zistenie úrovne rizík; analýza rizík poskytuje základ na vyhodnotenie rizík a rozhodnutie o spôsobe ich ošetrenia
bezpečnosť		ochrana fyzických a informačných aktív pred stratami, ktoré by mohli vzniknúť v dôsledku škodlivých udalostí a incidentov
bezpečnostné riziko		všeobecný výraz na označenie potenciálnej možnosti narušenia bezpečnosti
bezpečnostný incident		Udalosť, v rámci ktorej došlo ku strate integrity, alebo dôvernosti dát, zničeniu dát, prelomeniu integrity systému, alebo obmedzeniu, či odmietnutiu dostupnosti služby, priestupok, alebo riziko priestupku proti bezpečnostnej politike, prípadne proti akceptovateľnému použitiu bezpečnostných politík, alebo nesplnenie štandardných postupov.
dopad		hodnota závažnosti ujmy, resp. rozsah škody, ktorá môže byť spôsobená zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou
hrozba		Akákoľvek okolnosť či udalosť, ktorá môže potenciálne využiť zraniteľné miesto informačných, alebo fyzických aktív a spôsobiť negatívny následok (dopad)

[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

Pojem	Skratka	Výklad
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 dopad.
kybernetická odolnosť		schopnosť organizácie kontinuálne pokračovať v činnosti s najmenšou mierou narušenia aj v prípade kybernetického bezpečnostného incidentu, alebo inej škodlivej udalosti
kybernetické bezpečnostné riziko		riziko spôsobené narušením dôvernosti, integrity, dostupnosti, alebo sledovateľnosti informačných aktív organizácie, vytvorených, uložených, spracúvaných, alebo prenášaných informačnými technológiami
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 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		Aktivity vedúce k identifikácii, analýze, odozve na incident, odvráteniu hrozieb s úmyslom preventívne pôsobiť na možné opakovanie incidentu; návrh zrozumiteľného, predvídateľného a opakovateľného procesu odozvy na bezpečnostné incidenty
riziko		efekt neistoty dosiahnutia cieľa; pravdepodobnosť, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu, alebo škody;
rizikový apetít		ochota organizácie prijať riziká tak, ako sú kvantifikované príslušnými ukazovateľmi
tolerancia rizika		miera, do akej organizácia vyžaduje, aby boli jej informačné aktíva chránené pred hrozbami
úroveň rizika		závažnosť rizika vyjadrená ako kombinácia následkov a ich pravdepodobnosti
vlastník rizika		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.
zraniteľnosť		Slabé miesto fyzického, alebo informačného aktíva, slabé miesto v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať, alebo využiť nositeľ hrozieb (resp. hrozba, škodlivá udalosť, scenár rizika)

2. Proces riadenia rizika

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

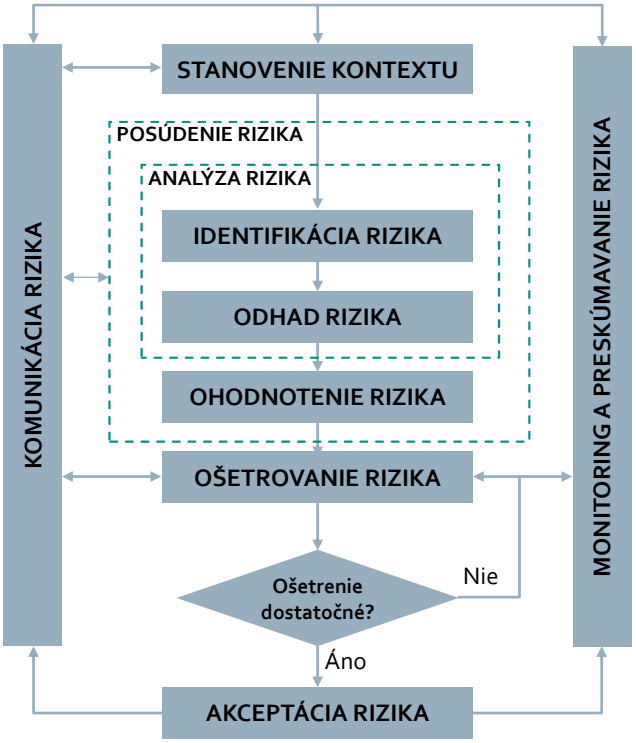
1. stanovenie kontextu rizík
2. posúdenie rizík
3. ošetrovanie rizík
4. komunikácia o rizikách
5. monitorovanie a preskúmanie rizika

Posudzovanie 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 ISO/IEC 27005:



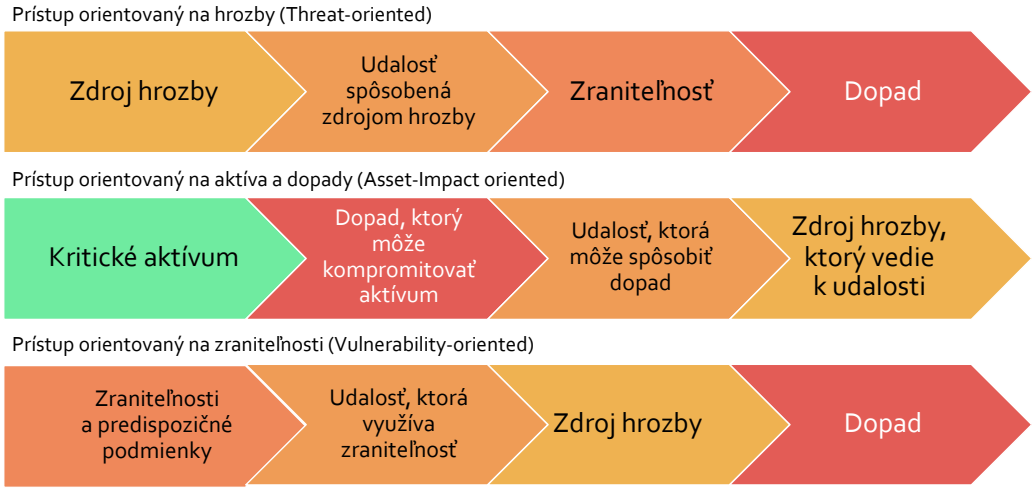
3. Metodika analýzy rizík

3.1. Alternatívne prístupy ku analýze rizika

Podľa NIST 800-39, NIST SP 800-30[3] existujú tri rôzne prístupy ku 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 dopady** (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 nepriaznivý vplyvom
- **Prístup orientovaný na zraniteľnosti** (z angl. Vulnerability-oriented)
  - Identifikuje predispozičné podmienky
  - Identifikujte zneužiteľné zraniteľnosti
  - Identifikujte hrozby v kontexte známych/identifikovaných zraniteľnosti

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



3.2. Metódy hodnotenia rizika

3.2.1. Kvalitatívne metódy

Na definovanie rizikových faktorov sú použité **nečíselné (slovné) hodnoty.** Hodnota pravdepodobnosti a dopadu 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.

Kvalitatívne metódy sa využívajú sa v prípadoch, ak chýbajú, alebo sú ťažko vyjadriteľné číselné hodnoty (údaje) pre kvantitatívne ohodnotenie rizika.

3.2.2. Kvantitatívne metódy

Na definovanie rizikových faktorov sú použité **numerické hodnoty.** Hodnota pravdepodobnosti, početnosti, vierohodnosti, potenciálu, dôsledkov, dopadu a pod je určená na základe histórie udalostí.

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

Tieto metódy sa dajú použiť predovšetkým v tých prípadoch, ak je k dispozícii dostatok relevantných údajov, ktoré sa dajú štatisticky vyhodnotiť.

3.2.3. Semikvantitatívne (zmiešané) metódy

Na definovanie rizikových faktorov je použitý **numerický rozsah hodnôt so slovne vyjadreným kontextom**. Hodnoty pravdepodobnosti a dopadu sú odvodené z rozsahu číselnej stupnice s priradením príslušného stupňa jedinečného významu.

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** analýze, v závislosti od potrieb organizácie, podľa legislatívnych požiadaviek[4] a podľa bezpečnostných štandardov.[5]

[4] Vyhláška UPVII č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy ako aj Vyhláška NBÚ č. 362/2018 ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

[5] STN ISO/IEC 27005 Riadenie rizík informačnej bezpečnosti

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 dopadov,
e) odhad pravdepodobností,
f) identifikácia existujúcich opatrení.

4.1. Identifikácia aktív a ich vlastníkov

Jednou zo základných úloh manažmentu každej organizácie je riadenie zdrojov, do ktorej patrí aj ochrana aktív. Prvým krokom pri ochrane týchto aktív je vytvorenie prehľadného zoznamu aktív a ich vlastníkov, ktorý je jedným z hlavných vstupov do analýzy rizík.

Za tvorbu a prispievanie do 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 Assessment“ – BIA), ako špecifická analýzy 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[6]. 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:

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

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 lokácie, aplikácie).

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

- 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
- ISO/IEC 27005 - poskytuje približne 60 hrozieb v 8 kategóriách
- Bundesamt fur Sicherheit in der Informatiionstechnik (BSI) IT- Grundschut-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
- Procesy riadenia IT služieb - riziká zistené pri nahlásení incidentu, alebo iného typu požiadavky na ServiceDesk, ktoré môžu identifikovať najmä zamestnanci IT,
- 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 dopad 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 dopadov

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

4.5. Identifikácia existujúcich opatrení

Pri výkone analýzy rizík je prostredie organizácie resp. nasadenia / prevádzky IS skúmané ako jeden celok, vrátane existujúcich opatrení. Tieto pri určovaní výslednej hodnoty rizika musia byť zohľadnené.

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.).

4.6. Závažnosť rizík

Ohodnotenie závažnosti rizík je vyjadrené stupňom podľa nasledovných sémantických významov:

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

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 hrozby, škodlivé udalosti alebo scenáre
   a) odhad pravdepodobnosti naplnenia hrozieb, škodlivých udalostí alebo ich kombinácie (tzv. scenárov rizík),
   b) odhad dopadov,
   c) určenie úrovne 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 ústiacimi do rôznych dopadov.[7]

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.

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 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.

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

5.3.1. Odhad pravdepodobnosti naplnenia scenára rizika

Určenie pravdepodobnosti naplnenia scenára rizika je požiadavkou na vyhodnotenie daného scenára rizika. Riziko s veľkým dopadom, ktoré sa však vyskytne iba raz za dlhý časový horizont môže mať menší negatívny vplyv na bezpečnosť ako riziko s nízkym dopadom, avšak s častejším výskytom. Poznať, resp. správne odhadnúť pravdepodobnosť výskytu je preto dôležitou súčasťou hodnotenia výsledného rizika. Do výslednej hodnoty pravdepodobnosti sú zohľadňované aj existujúce bezpečnostné opatrenia súvisiace s daným scenárom rizika.

Pri určovaní pravdepodobnosti naplnenia scenára rizika sa vychádza z jeho predpokladaného naplnenia v časovom horizonte dvoch rokov. V analýze rizík je táto pravdepodobnosť vyjadrená nasledujúcim rozsahom:

Pravdepodobnosť	Pravdepodobnosť popisne
Vysoká	je takmer isté, že v dohľadnom čase nastane naplnenie scenára rizika,
Stredná	je pravdepodobné, že v dohľadnom čase nastane naplnenie scenára rizika,
Nízka	je možné, že v dohľadnom čase nastane naplnenie scenára rizika
Veľmi nízka	je nepravdepodobné, že by v dohľadnom čase malo nastať naplnenie scenára rizika.

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.

5.3.2. Odhad dopadov pri naplnení scenára rizika

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

Dopad	Dopad popisne
Zanedbateľný	dopad akceptovateľného charakteru, ktorý môže byť zvládnutý v rámci plnenia bežných pracovných povinností bez potreby dodatočných zdrojov na odstránenie dôsledkov
Minimálny	dopad neakceptovateľného charakteru, ktorý však môže byť zvládnutý v rámci plnenia bežných pracovných povinností s minimálnymi personálnymi a finančnými nárokmi
Stredný	dopad neakceptovateľného charakteru, ktorý nie je zvládnuteľný v rámci plnenia bežných pracovných povinností a generuje mimoriadne personálne a finančné nároky (napr. zapojenie externých špecialistov a zdroje nad rámec bežného rozpočtu)
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,
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

5.3.3. Určenie úrovne rizika

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

Matica určenia úrovne výsledného rizika kvalitatívnou metódou:

Pravdepodobnosť	**Dopad**			
	Zanedbateľný	**Minimálny**	**Závažný**	**Katastrofický**
Vysoká	C	B	A	A
Stredná	C	B	B	A
Nízka	D	C	B	B
Veľmi nízka	D	D	C	C

Klasifikácia závažnosti rizika pri použití kvalitatívnej metódy vyplýva priamo z matice pre určenie úrovne výsledného rizika.

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 dopadu jednotlivých hrozieb v súvislosti s daným aktívom,
   c) výpočet úrovne závažnosti výsledných rizík,
   d) klasifikácia úrovní závažnosti rizík.

6.2. Stanovenie jednotného indexu rizika

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

Úroveň závažnosti	Dolný interval	Horný interval
Mimoriadne závažné	81	100
Vysoké	51	80
Nízke	21	50
Zanedbateľné	1	20

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.

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

6.3. Identifikácia relevantných zraniteľností a hrozieb

V zmiešanej metóde sa uplatňuje prístup orientovaný na aktíva a dopady (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 jej pravdepodobnosti a určiť hodnota dopadu 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 dopadu sú odvodené z rozsahu číselnej stupnice s priradením príslušného stupňa jedinečného významu.

6.4.1. Určenie hodnoty pravdepodobnosti hrozieb

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.

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

Pravdepodobnosť	**%**	**Frekvencia slovne**	**Pravdepodobnosť popisne**	**Hod-nota**
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**
Stredná	51 – 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**
Nízka	11 – 50	Niekedy	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.	**0,5**
Veľmi nízka	0 – 10	Málokedy	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľností. Neexistuje historická skúsenosť so zneužitím danej zraniteľnosti.	**0,1**

6.4.2. Určenie hodnoty dopadu hrozieb

Opis dopadu	Finančný dopad (príklad*)	Prevádzkový dopad	Dopad na súlad	Reputačný dopad	Hod-nota
Zanedbateľný	1 – 1500 €	Interne, jeden útvar	Zlyhanie interného procesu	Určité prekážky v komunikácii v rámci organizácie	**5**
Minimálny	1501 – 15 000 €	Interne, viacero útvarov	Zlyhanie kritických procesov	Prekážky v komunikácii v rámci organizácie	**20**
Stredný	15 001 – 150 000 €	Organizácia, malá časť klientov	Začatie správneho konania smerujúce k opatreniu na nápravu	Závažné prekážky v externej komunikácii	**50**
Závažný	150 001 – 1 500 000 €	Organizácia, značná časť klientov	Začatie správneho konania smerujúce k uloženiu pokuty	Nepriaznivá publicita, prípadne na národnej úrovni	**70**
Katastrofický	1 500 001 – 15 000 000 €	Organizácia, všetci klienti	Pozastavenie časti služieb / ukončenie činnosti	Intenzívna nepriaznivá publicita na národnej, alebo medzinárodnej úrovni	**100**

** Katastrofický dopad musí byť stanovený pre každú organizáciu individuálne a proporčne katastrofickému dopadu aj pre všetky nižšie úrovne dopadu*

6.4.3. Výpočet úrovne závažnosti rizík

Úroveň závažnosti rizika [R] je vyhodnocovaná ako násobok stanovenej pravdepodobnosti rizika [P] a stanoveného dopadu rizika [D]. Všeobecne je funkcia pre výpočet rizika v prístupe orientovanom na hrozby uvádzaná ako:

$$R = P \times D$$

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 vypočíta 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.:

$$R = \sum R_1 \ldots R_n$$

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

$$\overline{R_s} = \frac{1}{n} \sum_{i=1}^{n} R_i$$

Riziková expozícia informačného aktíva sa 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:

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

Výsledné hodnoty množiny je následne možné zaradiť v dvojrozmernej matici:

Pravdepodobnosť hrozby	**Dopad hrozby**				
	Zanedbateľný (5)	**Minimálny (20)**	**Stredný (50)**	**Závažný (70)**	**Katastrofický (100)**
Vysoká (1)	5*1,0=5	20*1,0=20	50*1,0=50	70*1,0=70	100*1,0=100
Stredná (0,8)	5*0,8=4	20*0,8=16	50*0,8=40	70*0,8=56	100*0,8=80
Nízka (0,5)	5*0,6=2,5	20*0,6=10	50*0,6=25	70*0,6=35	100*0,6=50
Veľmi nízkla (0,1)	5*0,1=0,5	20*0,1=2	50*0,1=5	70*0,1=7	100*0,1=10

6.4.4. Klasifikácia úrovne závažnosti rizík

Úroveň rizika číselne	**Úroveň závažnosti rizika slovne**	**Závažnosť rizika**
od 80 do 100	Mimoriadne vysoké	A
od 50 do 79	Vysoké	B
od 10 do 49	Nízke	C
od 0 do 9	Zanedbateľné	D

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

7. Ošetrovanie rizika

7.1. Metódy ošetrenia rizika

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

7.1.1. 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).

7.1.2. 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),

7.1.3. 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).

7.1.4. Zachovanie rizika

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

7.2. Návrh bezpečnostných opatrení

V zmysle všeobecných zásad tejto metodiky majú byť riziká byť 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:

Závažnosť rizika	Úroveň závažnosti rizika	Opatrenia
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 opatrení.
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.

Štruktúra opatrení podľa tejto metodiky je založená na štruktúre podľa Vyhlášky NBÚ č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

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.

7.2.1. 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.

7.2.2. 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 dopad hrozby na funkčnosť IS,
- zdokumentovať priebeh rizika.

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

8. Akceptácia zvyškového rizika

8.1. Zvyškové riziko

Zvyškové je také 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,
- 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.

8.2. 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

8.3. 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 na 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.

9. 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.

9.1. 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. [8]

Vzor správy o riziku je na v prílohe č.2.

[8] 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

10. Prílohy

10.1. 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		

10.2. 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		
Dopady	Identifikácia dopadov, ktoré môžu nastať po realizácii hrozieb		
Existujúce opatrenia			
1. opatrenie 2. opatrenie 3. opatrenie			
Úroveň dopadu	Hodnota dopadu	**Pravdepodobnosť naplnenia**	Hodnota pravdepodobnosti naplnenia
Výsledné riziko	**A B C D**		
Navrhované opatrenia			
1. opatrenie 2. opatrenie 3. opatrenie			