MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Metodika analýzy rizík a analýzy dopadov

Obsah

1 Správa dokumentu

Tento dokument je metodickým materiálom slúžiacim pre potreby orgánov verejnej moci, ktorý nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument je možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

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

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

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

2 Úvod

2.1 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“.

2.2 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 (Zákon č. 95/2019 Z. z. informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov).

2.3 Zásady navrhovanej metodiky

Tento dokument priamo vychádza a nadväzuje na Metodiku 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), ktorá bola vydaná Národným bezpečnostným úradom.

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.

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.

2.4 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 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy),
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy)
- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy),
- STN ISO 31000 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 (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).

3 Proces riadenia rizika

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

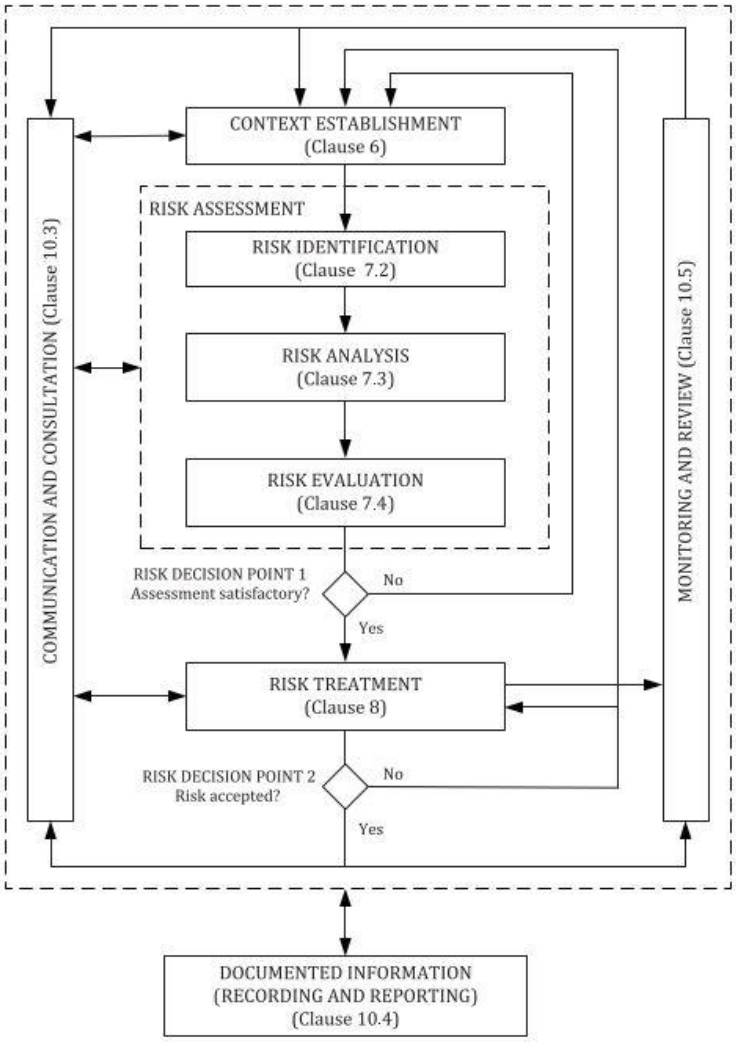
- stanovenie kontextu rizík,
- posúdenie rizík,
- ošetrovanie rizík,
- komunikácia o rizikách,
- monitorovanie a preskúmanie rizika.

Posudzovanie rizík je komplexný proces, ktorý pozostáva z:

- identifikácie rizík,
- analýzy rizík a
- 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 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy):



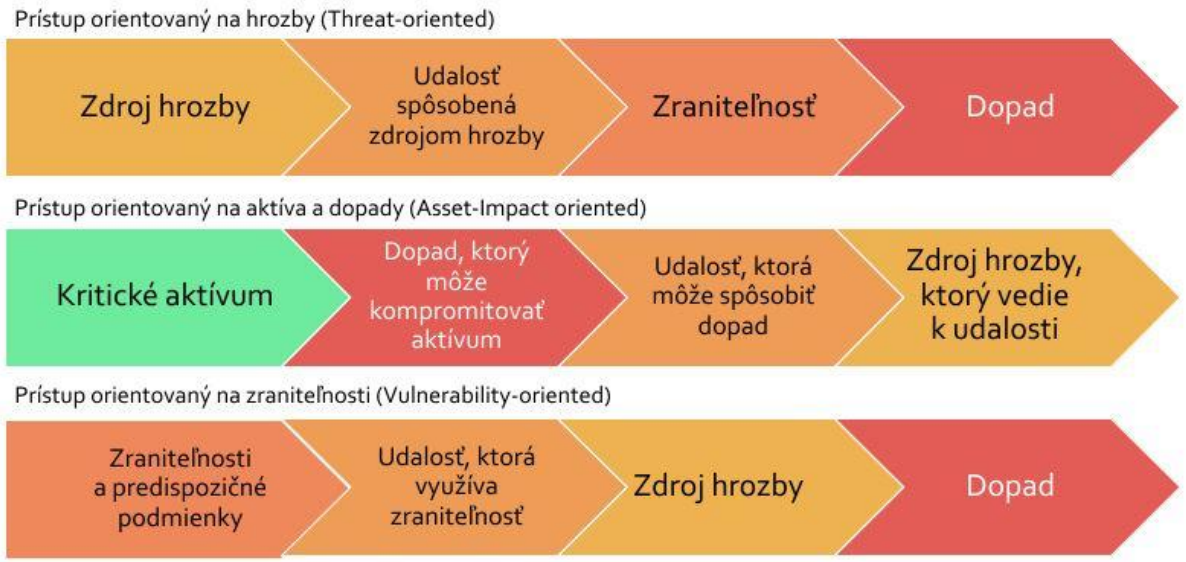
4 Metodika analýzy rizík

4.1 Alternatívne prístupy

Podľa NIST 800-39, NIST SP 800-303 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:



4.2 Kvalitatívna metóda hodnotenia rizika

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.

5 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:

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

5.1 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 hierarchie6. 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
Systémovo 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).

5.2 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.

5.2.1 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 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy) - poskytuje približne 60 hrozieb
- Bundesamt fur Sicherheit in der Informatiionstechnik (BSI) IT- Grundschut-Katalog: Poskytuje komplexný zoznam 370 hrozieb spolu s príkladmi pre každú z nich

5.2.2 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.).

5.3 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.

5.4 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.

5.5 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.).

5.6 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.

6 Kvalitatívna analýza rizík

6.1 Všeobecný popis fáz kvalitatívnej analýzy rizík

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

- identifikácia scenárov rizík
- vyhodnotenie výsledného rizika pre identifikované hrozby, škodlivé udalosti alebo scenáre
  - odhad pravdepodobnosti naplnenia hrozieb, škodlivých udalostí alebo ich kombinácie (tzv. scenárov rizík),
  - odhad dopadov,
  - určenie úrovne výsledných rizík.

6.2 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.

6.3 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.

6.3.1 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 opisne
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.

6.3.2 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

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

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 kybernetickej a informačnej bezpečnosti,
- 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 a informačnej 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 predpis (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 Metodika analýzy dopadov (BIA)

Analýzou dopadov sa identifikujú rôzne kategórie procesov organizácie, na základe ich kritickosti, ich vzájomné závislosti, analyzujú sa potenciálne dôsledky (škôd/strát) pri rôznych dobách trvania kritických situácií, stanovujú sa maximálne akceptovateľné doby prerušenia (MTO), minimálne ciele kontinuity podnikania (MBCO), cieľové časy obnovy (RTO) a cieľové body obnovy (RPO).

Analýza dopadov je súčasťou procesu riadenia kontinuity činností, ktorý identifikuje potenciálne dopady vyplývajúce z možného prerušenia činností a ktorého cieľom je pripraviť také postupy a vytvoriť také podmienky, ktoré zabezpečia v prípade krízovej situácie kontinuitu činností vo vopred stanovenom rozsahu a návrat k fungovaniu organizácie v normálnom režime, ktorý pozostáva z:

- Fáza 1 – Analýza (preskúmanie) organizácie,
- Fáza 2 – Určenie stratégie, predstavuje najmä výber opatrení (postupov) na zabezpečenie kontinuity činností, resp. obnovy zdrojov,
- Fáza 3 - Implementácia, zahŕňa prípravu plánov (BCP a DRP), zabezpečenie potrebných priestorových, materiálnych, technických, finančných a personálnych kapacít, ako aj informovanie a prípravu zamestnancov,
- Fáza 4 - Monitorovanie spočíva v pravidelnom každoročnom preverovaní pripravenosti organizácie zabezpečiť kontinuitu činností a obnovu zdrojov. Monitorovanie zahŕňa najmä testovanie BCP a DRP a ich aktualizáciu.

Cieľom analýzy dopadov je najmä:

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

Analýza dopadov je v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov súčasťou bezpečnostnej dokumentácie. Výsledky analýzy dopadov slúžia ako vstup pre vypracovanie plánu kontinuity.

10.1 Fázy výkonu analýzy dopadov na činnosti organizácie

Výkon analýzy dopadov je štruktúrovaný do nasledujúcich hlavných fáz:

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

10.2 Spôsob zberu vstupných dát

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

Po stretnutí sa vyplnený dotazník zašle na validáciu zodpovedným osobám. V prípade komentárov a požadovaných zmien sa podľa povahy tieto zapracujú, alebo sa uskutoční ďalšie moderované stretnutie po dohode so zodpovednými osobami za činnosti alebo procesy.

10.3 Dotazník pre analýzu dopadov na činnosti organizácie

10.3.1 Základné informácie o procese

Medzi základné informácie o procese, ktoré budú v dotazníku zachytené patria:

- názov procesu,
- organizačná jednotka, pod pôsobnosť ktorej daný proces spadá,
- vlastník procesu,
- príslušná činnosť, pre zabezpečenie ktorej je daný proces nevyhnutný,
- typy informácií / dokumentov spracúvaných v danom procese,
- krátky popis činností vykonávaných v procese.

10.3.2 Väzby a závislosti procesu

V tejto časti sú identifikované závislosti analyzovaného procesu na:

- podprocesoch, čiže procesoch, pre ktoré je daný proces nadradený,
- informačných systémoch, aplikáciách a komunikačných službách,
- iných procesoch, ktorých výstupy sú vstupy potrebné pre daný proces,
- externých dodávateľoch (kto a aké služby a tovary poskytuje)

a väzby na:

- klientov,
- regulátorov (predmet regulácie, rôzne termíny na zasielanie výkazov a pod.).

10.3.3 Profil vykonávanej práce

Profil vykonávanej práce znamená identifikácia:

- kritického obdobia,
- množstva práce vykonávanej v kritickom období,
- minimálneho prijateľného množstva práce vykonávanej bezprostredne po krízovej situácii,
- či môže definovaný typ krízovej situácie spôsobiť prerušenie procesu.

Typmi uvažovaných krízových situácií sú:

- nedostupnosť informačných technológií a/alebo dát,
- nedostupnosť prevádzkových priestorov,
- nedostupnosť kritickej časti ľudských zdrojov - zamestnancov,
- zlyhanie kľúčového externého dodávateľa služieb.

Kritické obdobie

Kritické obdobie je obdobie v dni, týždni, mesiaci a / alebo roku, kedy je kontinuita procesu najkritickejšia, čiže proces je najcitlivejší a dopady v prípade kritickej situácie sú najvyššie. V prípade, že proces má stále rovnakú kritickosť / citlivosť na dopady, tak sa uvedie *každý pracovný deň* alebo *každý kalendárny deň*.

Množstvo práce vykonávanej v kritickom období

Množstvo práce, ktoré sa vykonáva v definovanom kritickom období znamená napríklad množstvo výrobkov alebo služieb, počet spracovaných položiek, transakcií a pod. za určitú jednotku času.

Minimálne prijateľné množstvo práce vykonávanej bezprostredne po krízovej situácie

Množstvo práce, ktoré sa má vykonávať bezprostredne po krízovej situácii znamená napríklad množstvo výrobkov alebo služieb, počet spracovaných položiek, transakcií atď. za určitú jednotku času. Je to definícia minimálnej úrovne činnosti/procesu, ktorá sa má zachovať bezprostredne po kritickej situácii, inými slovami definícia Minimálne ciele kontinuity podnikania (MBCO).

10.3.4 Funkčné dopady

V tejto časti sa kvalitatívne hodnotí výška funkčného dopadu krízovej situácie, v týchto oblastiach:

- strata reputácie,
- strata klientov / žiadateľov,
- dopad na iné činnosti organizácie,
- dopad na zdravie, bezpečnosť a prostredie.

Výška funkčného dopadu sa určuje zvlášť pre rôzne dĺžky trvania krízovej situácie. Rôzne dĺžky trvania krízovej situácie, pre ktoré sa budú hodnotiť dopady, budú definované na stretnutiach s vlastníkmi procesov.

Samotná hodnota funkčného dopadu sa určí podľa nasledovnej stupnice:

Bezvýznamný dopad	1	Trvanie krízovej situácie spôsobuje zanedbateľné poškodenie.
Akceptovateľný dopad	2	Trvanie krízovej situácie spôsobuje škodu, ale táto škoda je prijateľná vzhľadom na jej veľkosť a špecifické okolnosti.

Vysoký dopad	3	Trvanie krízovej situácie spôsobuje škodu, ktorá je neprijateľná pre svoju veľkosť a špecifické okolnosti.
Kritický dopad	4	Trvanie krízovej situácie spôsobuje veľmi vysokú škodu na reputácii organizácie, iných činnostiach organizácie alebo zdraví, bezpečnosti a prostredia a / alebo organizácia bude musieť natrvalo ukončiť svoju činnosť.

10.3.5 Finančné dopady

V tejto časti sa kvantitatívne hodnotí výška priameho finančného dopadu krízovej situácie, v týchto oblastiach:

- priame finančné škody,
- sankcie regulačných orgánov,
- zmluvné pokuty a / alebo uplatnenie náhrady škôd zo strany zmluvných partnerov,
- náklady súvisiace s návratom do normálneho stavu.

Výška finančného dopadu sa určuje zvlášť pre rôzne dĺžky trvania krízovej situácie. Rôzne dĺžky trvania krízovej situácie, pre ktoré sa budú hodnotiť dopady, budú definované na stretnutiach s vlastníkmi procesov.

Samotná hodnota finančného dopadu sa určí sumou v EUR.

10.3.6 Strata údajov

V tejto časti sa kvalitatívne hodnotí výška dopadu straty údajov vyvolanej krízovou situáciou. Samostatne sa hodnotí maximálne množstvo údajov, ktoré sa môže stratiť v týchto formách:

- aplikácie, databázy,
- elektronické údaje, ktoré nie sú uložené v databázach (čiže napríklad údaje uložené na rôznych nosičoch ako CD, USB a pod.),
- papierové dokumenty.

Rôzne dopady sa posudzujú pre rôznu stratu údajov, podľa množstva údajov, ktoré sa vytvorili v poslednom časovom úseku. Jednotlivé časové úseky, pre ktoré sa budú hodnotiť dopady, budú definované na stretnutiach s vlastníkmi procesov.

Samotná hodnota dopadu straty údajov sa určí podľa nasledovnej stupnice:

Bezvýznamný dopad	1	Množstvo stratených údajov spôsobuje zanedbateľné finančnú škodu alebo zanedbateľnú škodu na právnych alebo zmluvných záväzkoch, reputácii organizácie, iných činnostiach organizácie alebo zdraví, bezpečnosti a prostredia.
Akceptovateľný dopad	2	Množstvo stratených údajov spôsobuje finančnú škodu, alebo škodu na právnych alebo zmluvných záväzkoch, reputácii organizácie, iných činnostiach organizácie alebo zdraví, bezpečnosti a prostredia, ale táto

		škoda je prijateľná vzhľadom na jej veľkosť a špecifické okolnosti.
Vysoký dopad	3	Množstvo stratených údajov spôsobuje finančnú škodu, alebo škodu na právnych alebo zmluvných záväzkoch, reputácii organizácie, iných činnostiach organizácie alebo zdraví, bezpečnosti a prostredia, ktorá je neprijateľná pre svoju veľkosť a špecifické okolnosti.
Kritický dopad	4	Množstvo stratených údajov spôsobuje finančnú škodu, alebo škodu na právnych alebo zmluvných záväzkoch, reputácii organizácie, iných činnostiach organizácie alebo zdraví, bezpečnosti a prostredia, ktorá spôsobí veľmi vysokú finančnú stratu pre organizáciu a / alebo organizácia bude musieť natrvalo ukončiť svoju činnosť.

10.3.7 Identifikácia zdrojov a prostriedkov na obnovu procesu

Identifikácia zdrojov a prostriedkov na obnovu procesu sa bude vykonávať iba pre procesy, ktoré majú zásadný vplyv na kontinuitu činností organizácie. Tieto procesy budú identifikované v rámci analýzy, na základe ich hodnoty RTO.

Pre analyzovaný proces je potrebné identifikovať nasledovné typy zdrojov a prostriedkov pre obnovu procesu:

- ľudia:
  - je potrebné uviesť aj vzdelanie, zručnosti, role atď.,
- aplikácie, databázy:
  - je potrebné uviesť počty užívateľov,
- elektronické údaje, ktoré nie sú uložené v databázach (napríklad údaje uložené na rôznych nosičoch ako CD, USB a pod.),
  - je potrebné uviesť aký typ a aj kde sú uložené,
- papierové dokumenty:
  - je potrebné uviesť aký typ a aj kde sú uložené,
- priestory:
  - je potrebné uviesť kapacitu, technické špecifikácie,
- kancelárske a komunikačné vybavenie:
  - vrátane IT vybavenia, komunikačného vybavenia (kapacity),
- externí dodávatelia:
  - je potrebné uviesť službu/tovar a meno spoločnosti, ktorá ju organizácii poskytuje

a to zvlášť pre jednotlivé časové úseky od výskytu krízovej situácie.

Rôzne časové úseky od výskytu krízovej situácie, pre ktoré sa budú identifikovať zdroje, budú definované na stretnutiach s vlastníkmi procesov.

Pre každý zdroj alebo prostriedok je potrebné určiť:

- počet zdrojov alebo prostriedkov, ktoré sú potrebné na obnovenie činnosti,
- čas, po ktorom je zdroj alebo prostriedok požadovaný (čas od výskytu krízovej situácie).

10.3.8 Alternatívny poskytovateľ procesu

Pre analyzovaný proces treba identifikovať alternatívneho poskytovateľa tohto procesu (ak existuje) v prípade vzniku krízovej situácie.

Pre každého identifikovaného alternatívneho poskytovateľa procesu treba uviesť :

- či je riešenie interného alebo externého charakteru,
- v prípade, že sa jedná o interného poskytovateľa, treba uviesť názov organizačnej jednotky a v prípade externého poskytovateľa treba uviesť meno organizácie,
- či sa jedná o ručné alebo automatizované vykonávanie alternatívneho riešenia,
- rozsah pokrytia pôvodného procesu alternatívnym riešením, t. j. na koľko percent by alternatívny poskytovateľ bol schopný pokryť daný proces (napríklad percento spracovaných formulárov a pod.),
- akceptovateľné trvanie, t. j. počet hodín do kedy by bolo identifikované alternatívne riešenie prijateľné/možné.

Ak neexituje žiadny alternatívny poskytovateľ procesu, uvedie sa *N/A*.

10.3.9 Predchádzajúce skúsenosti s krízovými situáciami

V záverečnej časti zodpovedné osoby uvedú predchádzajúce skúsenosti s krízovými situáciami, ktoré ovplyvnili alebo mohli ovplyvniť kontinuitu analyzovaného procesu, ako často sa také situácie vyskytujú, ako dlho trvali, a ako sa s nimi vysporiadali.

10.4 Výstupy z analýzy dopadov na činnosti organizácie

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

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

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

10.4.1 Stanovenie hodnôt MTO, MBCO, RTO, RPO

Stanovenie hodnoty MTO

MTO činnosti sa stanoví priamo počas konkrétneho stretnutia, kde sa bude obchodná činnosť analyzovať.

Stanovenie hodnoty MBCO

MBCO činnosti sa identifikuje priamo počas konkrétneho stretnutia, kde sa bude činnosť analyzovať v rámci identifikácie minimálneho prijateľného množstva práce vykonávanej bezprostredne po krízovej situácii.

Stanovenie hodnoty RTO

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

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

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

Stanovenie hodnoty RPO

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

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

11 Prílohy

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		

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			