Bezpečnostný projekt
(metodika spracovania bezpečnostného projektu)

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. Dokument je potrebné upraviť na základe reálnych potrieb a špecifického prostredia organizácie.

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

2 Manažérske zhrnutie

Bezpečnostný projekt informačného systému verejnej správy (ďalej „ISVS“)je vytvorený správcom informačného systému (ďalej len „IS“) a tvorí súčasť bezpečnostnej dokumentácie vzhľadom na legislatívne požiadavky zákona č. 95/2019 Z. z.o informačných technológiách vo verejnej správe o zmene a doplnení niektorých zákonov a jeho vykonávacích predpisov pre potreby informačného systému verejnej správy najmä vyhlášky 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 (Príloha č. 3). Vypracovanie bezpečnostného projektu informačného systému verejnej správy zabezpečí správca, vychádzajúc:

- zo stratégie kybernetickej bezpečnosti a bezpečnostných politík,
- zo všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajú z uznaných technických noriem,
- z metodických usmernení orgánu vedenia.

Správca vypracuje bezpečnostný projekt pre informačný systém verejnej správy, ktorý:

- pri narušení bezpečnosti môže spôsobiť závažný kybernetický bezpečnostný incident,
- tvorí základné registre alebo referenčné registre alebo je ich súčasťou,
- je agendový informačný systém,
- je nevyhnutný na rozhodovanie orgánu verejnej moci,
- je špecializovaný portál,
- spracúva osobitné kategórie osobných údajov podľa osobitného predpisu,
- je zaradený do kategórie III. podľa osobitného predpisu.

Bezpečnostný projekt IS definuje formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov organizácie, technických noriem a štandardov dobrej praxe. Dokument obsahuje komplexné posúdenie bezpečnostných potrieb, určenie bezpečnostných požiadaviek, návrh spôsobu ich efektívneho naplnenia a vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika.

Bezpečnostný projekt slúži na eliminovanie a minimalizovanie rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti. Správca tohto informačného systému chráni spracúvané informácie pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania.

Pri každom riziku sa zohľadňuje pravdepodobnosť situácie, pri ktorej hrozby využijú existujúce zraniteľnosti a spôsobia negatívny vplyv na aktíva orgánu riadenia. Pri hodnotení závažnosti výsledného vplyvu sa zohľadňuje celková závažnosť vplyvov, ktoré môžu byť spôsobené pri realizácii rizika. Úroveň vplyvov sa určuje osobitne pre každé analyzované riziko a zahŕňa všetky aktíva dotknuté príslušným rizikom. Analyzované riziko môže mať na aktíva orgánu riadenia viaceré vplyvy, ktoré je potrebné sumárne vyhodnotiť a zdokumentovať. Výsledná miera rizika musí zohľadňovať aj všetky realizované bezpečnostné opatrenia.

Na tento účel sú prijímané primerané technické, organizačné a personálne opatrenia zodpovedajúce

spôsobu spracúvania informácií, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných informácií, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému. Prijatím bezpečnostných opatrení správca neoprávneným osobám znemožňuje akýkoľvek nedovolený prístup k spracúvaným informáciám a oprávneným osobám zabezpečí prístup k informáciám v rozsahu potrebnom na plnenie ich povinností.

Tento dokument je určený správcom IS, manažérom kybernetickej a informačnej bezpečnosti a tým, ktorí budú zapojení do prípravy bezpečnostného projektu.Za udržiavanie a aktuálnosť tohto bezpečnostného projektu zodpovedá správca IS.

3 Ciele bezpečnostného projektu IS

Cieľom tohto bezpečnostného projektu IS je definovanie základných rámcov ochrany informácií spracúvaných počas celého ich životného cyklu, t.j. od ich získavania až po ich likvidáciu, so zabezpečením súladu dôvernosti, integrity a dostupnosti informácií.

Súčasťou tohto bezpečnostného projektu IS je analýza rizík, ktorou sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva.

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.

Analýza rizík je zároveň určená ako fundamentálny podklad pre spracovanie Bezpečnostného projektu konkrétnych IS. V tomto formáte potom slúži na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti. Analýza rizík je hlavnou časťou bezpečnostného projektu vytvoreného pre správcu IS v kontexte požiadaviek zákona č. 95/2019 Z. z.a jeho vykonávacích predpisov pre potreby informačného systému verejnej správy. Bezpečnostný projekt IS potom definuje formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov organizácie, technických noriem a štandardov dobrej praxe (obsahuje komplexné posúdenie bezpečnostných potrieb, určenie bezpečnostných požiadaviek, návrh spôsobu ich efektívneho naplnenia a vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika).

Analýzou rizík sa identifikujú a ohodnocujú riziká, ktoré majú alebo môžu mať na chránené informačné aktíva vplyv. Výstupy takejto analýzy pomôžu v rozhodovaní vedeniu organizácie a zodpovedných pracovníkov pri aplikovaní bezpečnostných opatrení.

4 Štruktúra bezpečnostného projektu IS

Konkrétny obsah a štruktúra bezpečnostného projektu ISVS je povinná v kontexte požiadavky platnej legislatívy a je detailne uvedená v **Prílohe č. 3** k vyhláške č. 179/2020 Z. z.

Pri spracovaní bezpečnostného projektu informačného systému verejnej správy sa prihliada najmä na zložitosť informačného systému verejnej správy, komplexnosť agendy pokrytej informačným systémom verejnej správy a stanovenie bezpečnostných požiadaviek na informačný systém verejnej správy. Zohľadniť sa musí taktiež kategória, do ktorej je informačný systém verejnej správy zaradený.

Bezpečnostný projekt informačného systému verejnej správy pozostáva z dvoch hlavných výstupov (komponentov):

a) bezpečnostný zámer (jedná sa o prvý výstup bezpečnostného projektu informačného systému verejnej správy, ktorý určuje najmä kontext a zameranie bezpečnostného projektu, preto v súlade s legislatívou (Príloha č. 3 k vyhláške č. 179/2020 Z. z.),

b) analýza bezpečnosti (súčasťou dokumentu „Analýza bezpečnosti“ je analýza rizík. Rizikom sa v bezpečnostnom projekte chápe miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami).

4.1 Bezpečnostný zámer

Táto kapitola bezpečnostného projektu obsahuje:

- formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov orgánu riadenia, technických noriem a štandardov dobrej praxe,
- zoznam právnych predpisov aplikovaných v bezpečnostnom projekte, ako aj interných riadiacich aktov,
- metodický prístup ku kvalitatívnej analýze rizík, ktorá je v bezpečnostnom projekte vykonaná,
- rámcovú špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany informačného systému verejnej správy, jeho služieb a údajov v ňom spracúvaných s ohľadom na kategóriu, do ktorej je informačný systém verejnej správy zaradený,
- vymedzenie okolia informačného systému verejnej správy a jeho vzťah k možnému narušeniu bezpečnosti informačného systému verejnej správy vrátane zoznamu integrácií na informačný systém verejnej správy,
- vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,
- ohraničenia bezpečnostného projektu (explicitné vysvetlenie oblastí, ktoré bezpečnostný projekt nezahŕňa alebo kladie požiadavky na ich riešenie mimo projektu informačného systému verejnej správy),
- postupy revízie/aktualizácie bezpečnostného zámeru.

Hlavnými strategickými bezpečnostnými cieľmi z pohľadu kybernetickej a informačnej bezpečnosti sú:

- Kybernetická a informačná bezpečnosť ako základná súčasť DNA organizácie
- Dôveryhodná organizácia pripravená na hrozby

- Riadiť kybernetickú a informačnú bezpečnosť v súlade s požiadavkami platnej legislatívy SR aj EÚ, medzinárodnými štandardmi a odporúčaniami odvetvovej praxe
- Zabezpečovať primeranými technickými, organizačnými a personálnymi bezpečnostnými opatreniami ochranu dôvernosti, integrity a dostupnosti informačných aktív
- Zabezpečovať primeranými technickými, organizačnými a personálnymi opatreniami ochranu informácií v informačných systémoch, vrátanie osobných údajov pred odcudzením, nedostupnosťou, poškodením, neoprávneným prístupom, zmenou a rozširovaním
- Implementovať a udržiavať plán reakcie na kybernetické bezpečnostné incidenty
- Podieľať sa na zaistení kontinuity činností spoločnosti v prípade kybernetických bezpečnostných incidentov
- Zvyšovať povedomie o informačnej a kybernetickej bezpečnosti všetkých zamestnancov a vedenia inšitúcie
- Riadiť riziká kybernetickej a informačnej bezpečnosti s cieľom implementovať efektívne opatrenia na ich minimalizáciu
- Zaistiť bezpečnú prevádzku a správu informačných systémov
- Zabezpečiť dôvernosť, dostupnosť a integritu najmä osobných údajov, obchodného tajomstva a iných dôležitých informačných aktív organizácie, fyzických a právnických osôb pri ich spracúvaní
- Minimalizácia finančných a iných strát súvisiacich s narušením prevádzky informačných systémov
- Zaistenie poskytovania služieb informačného systému užívateľom informačného systému v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch informačného systému
- Ochrana dobrého mena organizácie

4.2 Analýza bezpečnosti

Analýza bezpečnosti je jedným z hlavných výstupov bezpečnostného projektu.

Výstupný dokument analýzy bezpečnosti s výsledkami kvalitatívnej analýzy rizík obsahuje najmä:

- ciele a priority analýzy rizík,
- opis použitej metodiky analýzy rizík,
- opis rizík založený na identifikácii aktív, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností a na identifikácii vplyvov na aktíva najmä v dôsledku straty dôvernosti, integrity a dostupnosti,
- vyhodnotenie rizík podľa použitej metodiky,
- opis navrhovaných bezpečnostných opatrení pre identifikované riziká v závislosti od ich závažnosti,
- celkové zhrnutie výsledkov analýzy rizík, vrátane zoznamu vysokých a stredných rizík usporiadaných podľa dôležitosti, s opisom navrhovaného postupu ich riadenia a kľúčových navrhovaných bezpečnostných opatrení,

- postupy revízie / aktualizácie analýzy bezpečnosti.

4.3 Štruktúra dokumentu bezpečnostného projektu

Na základe dobrej praxea skúseností pri tvorbe predmetného dokumentu je nižšie uvedený jeden z možných spôsobov (návrh), ako by bezpečnostný projekt mohol vyzerať na úrovni konkrétnych kapitol (možné rozvrhnutie / štruktúra konkrétneho dokumentu):

I. Základné identifikačné údaje dokumentu - bezpečnostného projektu IS *(názov, číslo, vydanie, revízia, počet strán, gestor, vlastník, autor, kontrolór, schvaľovateľ, manažér kybernetickej a informačnej bezpečnosti)*

II. Zmenový list

III. Súvisiace dokumenty

IV. Použitá terminológia a skratky

V. Zoznam právnych predpisov

VI. Účel bezpečnostného projektu IS

VII. Ciele bezpečnostného projektu IS

VIII. Bezpečnostný zámer *(základné bezpečnostné ciele)*

IX. Analýza bezpečnosti

a) Metodika kvalitatívnej analýzy rizík *(identifikácia aktív, klasifikácia aktív, identifikácia a ohodnotenie bezpečnostných hrozieb, identifikácia a ohodnotenie bezpečnostných zraniteľností podľa hrozieb pôsobiacich na aktíva, ohodnotenie rizík)*

b) Samotná analýza rizík *(Výstupný dokument analýzy rizík)*

X. Navrhované bezpečnostné opatrenia

XI. Určenie nepokrytých rizík

XII. Vymedzenie kritérií na akceptáciu rizika

XIII. Ohraničenia aktíva, pre ktoré je analýza rizík spracovaná

XIV. Postupy revízie analýzy rizík

4.4 Zoznam právnych predpisov aplikovaných v bezpečnostnom projekte

Zoznam právnych predpisov aplikovaných v bezpečnostnom projekte:

- smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii – smernica NIS,
- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „zákon o kybernetickej bezpečnosti“),
- vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
- vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné

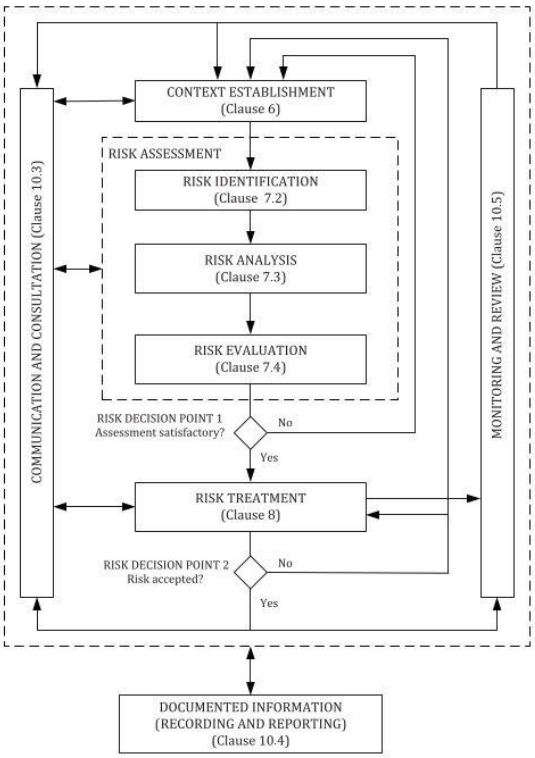
kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,

- vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
- zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) – GDPR,
- zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- autorský zákon č. 185/2015 Z. z. v znení neskorších predpisov.
- 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 (NBÚ)

5 Správa rizík

Správa rizík spočíva v tom, že organizácia popíše vonkajšie a vnútorné súvislosti (kontext, vplyvy) v rámci svojej činnosti (analyzovaných oblastí), ďalej ohodnotí riziká vyplývajúce z hrozieb voči svojim aktívam, ošetrí aspoň najzávažnejšie riziká prijatím opatrení, ktoré implementuje, a bude sledovať účinnosť prijatých opatrení.

Správa rizík je podrobne popísaná v rámci medzinárodného štandardu 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).



Obrázok 1.
Proces manažmentu rizík informačnej bezpečnosti

5.1 Prípravná fáza - stanovenie kontextu

Ak sa jedná o spracovanie prvého bezpečnostného projektu, je potrebné zmapovať stav bezpečnosti v organizácii – t. j. identifikovať hlavné aktíva, hrozby, bezpečnostné požiadavky a existujúce postupy a navrhnúť, čo by organizácia mala spraviť, aby od neusporiadaného bezpečnostného procesu prešla k systematickému riadeniu informačnej a kybernetickej bezpečnosti. Je nevyhnuté identifikovať bezpečnostné problémy a navrhnúť ich riešenie.

Kontextom sú pravidlá, obmedzenia a požiadavky, ktoré platia v celej organizácii a ktoré špecifický projekt musí zohľadňovať.

V ďalšom kroku je potrebné špecifikovať základné kritériá, rozsah a hranice a organizáciu procesu správy rizík.

Základné kritériá sú:

- kritéria vyhodnotenia rizík - tie vychádzajú z hodnoty aktív, kritickosti aktív, právnych požiadaviek na ochranu aktív a zmluvných záväzkov, dôležitosti dostupnosti, integrity a dôvernosti (možné negatívne dopady na dobré meno organizácie, klasifikácie aktív, a pod.),

- dopadové kritériá (vyjadrujú stupeň negatívnych dôsledkov spôsobených naplnením hrozby),
- kritériá pre akceptovanie rizík (výsledkom by mala byť hodnota akceptovateľného rizika).

Oblasť pôsobnosti a hranice

- Bezpečnostný projekt a správa rizík sa podľa požiadavky zákona č. 95/2019 Z. z. vzťahuje na celú organizáciu (s výnimkou utajovaných skutočností, prípadne iných špecifických oblastí). Je potrebné vymedziť vonkajšie prostredie, s ktorým organizácia interaguje, aby sa pri analýze rizík zohľadnili vonkajšie hrozby aj oprávnené požiadavky externých subjektov.
- V prípade, ak sa bezpečnostný projekt spracúva pre konkrétny informačný systém organizácie,sa správa rizík vzťahuje na konkrétny informačný systém. Správa rizík sa potom sústreďuje na aktíva predmetného informačného systému, pričom zohľadňuje aj jeho bezpečnostné okolie, skúma riziká a jehobezpečnostné okolie.

Organizácia manažmentu rizík

V tejto oblasti je vhodné stanoviť, aký spôsob riadenia rizík si organizácia zvolí tak, aby jej to vyhovovalo v praxi (t.j. aké povinnosti v organizácii vzniknú, keď sa začne systematicky zaoberať správou rizík a kto by tieto povinnosti mal vykonávať).

5.2 Ohodnotenie rizík

5.2.1 Identifikácia aktív

Organizácia potrebuje vedieť, čo potrebuje chrániť – je potrebné spracovať zoznam aktív a pre každé aktívum priradiť vlastníka.Výstupom by mali byť dva zoznamy – **zoznam aktív**a **zoznam činností (agiend)**, v ktorých sa aktíva používajú.

Podrobne uvedené v **Prílohe - identifikácia aktív**.

5.2.2 Identifikácia hrozieb

Hrozba je potenciálna možnosť narušenia aktíva organizácie. Príkladom je hrozba krádeže, kde je nositeľom hrozby osoba (zlodej), aktívom (objektom hrozby) mobilný telefón a zraniteľnosťou, že ho majiteľ nosí napr. v otvorenej taške.

Hrozby môžu byť neúmyselné (prírodný vplyv, technická porucha, ľudská chyba) alebo úmyselné (útok).

Podrobne uvedené v **Prílohe - zoznam hrozieb**.

5.2.3 Identifikácia zraniteľností

Existujú okolnosti, ktoré umožňujú naplnenie hrozieb voči aktívu. Samotná zraniteľnosť nestačí na poškodenie aktíva, na to musí existovať hrozba a jej nositeľ (preto je potrebné monitorovať aj doteraz neškodné zraniteľnosti).

Výstupom je zoznam zraniteľností spolu s relevantnými aktívami, hrozbami a opatreniami.

Podrobne uvedené v **Prílohe - zoznam zraniteľností**.

5.2.4 Identifikácia existujúcich opatrení

Opatrenie je vo všeobecnosti riešenie (organizačné, technické, fyzické, právne), ktoré zníži pravdepodobnosť toho, že dôjde k naplneniu hrozby voči aktívu, resp. zníži dopad naplnenia hrozby. Organizácia musí inventarizovať existujúce opatrenia minimálne aby sa:

- nezohľadňoval by sa vplyv existujúcich opatrení, keď bude stanovovať hodnotu rizík (mohlo by dôjsť k skresleniu výsledkov);
- pri implementácii nových opatrení mohlo posúdiť, či má zmysel ponechať staré opatrenia (neúčinnosť, redundancia, nekompatibilita, prevádzkové náklady).

Výstupom je zoznam existujúcich a plánovaných opatrení a ich stav (plánované/aktívne).

5.2.5 Identifikácia dopadov

V tejto časti je potrebné určiť dôsledky narušenia dôvernosti, integrity a dostupnosti pre aktíva.Prakticky to znamenáuvažovať nad možnými scenármi naplnenia hrozieb voči aktívam a zistiť, na čo všetko by naplnenie hrozby malo dopad.

5.3 Analýza rizík

Analýza rizík je zameraná na získanie aktuálnych a vierohodných poznatkov o pravdepodobných rizikách týkajúcich sa aktív informačného systému verejnej správy a jeho okolia. Analýza rizík sa vykonáva pre informačný systém verejnej správy priebežne počas celého projektu v súlade so zákonom č. 95/2019 Z. z. a priamo nadväzuje na dokument „Bezpečnostný zámer“ (resp. je jeho súčasťou).

Pre správnu analýzu rizík nestačí iba poznať hrozby,zraniteľnosti a dopady na aktíva. Chýbajúci faktor pri posudzovaní závažnosti nebezpečenstva, pred ktorým je aktíva organizácie potrebné chrániť, je pravdepodobnosť naplnenia hrozby.

Riziko je veličina spájajúca pravdepodobnosť naplnenia hrozby a dopad hrozby. Následne, po vyjadrení hodnoty rizík, je potrebné zamerať sa na ošetrenie rizík s najväčšou hodnotou a optimalizovať využívanie zdrojov.

Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti je podrobne spracovaná v materiály, publikovanom Národným bezpečnostným úradom**tu**.

V materiály je podrobne popísaná oblasť:

a) procesu a metodiky riadenia rizík,

b) stanovenia kontextu rizika (identifikácia aktív, hrozieb, zraniteľností, dopadov, existujúcich opatrení a závažnosti rizík),

c) kvalitatívnej analýzy rizík,

d) ošetrovania rizík vrátane návrhu bezpečnostných opatrení,

e) akceptácie zvyškového rizika,

f) komunikácie rizika.

Súčasťou dokumentu sú aj prílohy (Vzor návrhu na akceptáciu rizika, Vzor správy o riziku).

5.3.1 Kvalitatívna analýza rizík

Metodika kvalitatívnej analýzy rizík 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.

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.

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.

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.

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

6 Záver

Tento dokument popisuje a vysvetľuje záväzné postupy uvedené vo vyhláške 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.

Taktiež opisuje správu a riadenie rizík definované v rámci medzinárodnej 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) a dopĺňa riešenia, ktoré môžu zjednodušiť najmä analýzu rizík rozsiahlych organizácií a systémov.

Zavedenie systému riadenia kybernetickej a informačnej bezpečnosti (KIB) v organizácii by malo byť zahájené vysokoúrovňovou kvalitatívnou analýzou rizík. Tá umožní zistiť stav KIB v organizácii, identifikovať hlavné aktíva, ich zraniteľnosti, hrozby voči nim a odhadnúť riziká.

Na základe týchto informácií organizácia môže stanoviť svoju stratégiu v KIB a spracovať ju vo forme Politiky KIB (bezpečnostného zámeru, tvoriaceho prvú časť Politiky KIB), kde stanoví svoje hlavné ciele a rámcovo vymedzí spôsoby, akými chce tieto ciele dosiahnuť.

Samotná bezpečnosť kritických aktív organizácie sa rieši prostredníctvom bezpečnostného projektu, ktorého súčasťou je aj podrobná analýza rizík a návrh bezpečnostných opatrení. Časť bezpečnostných opatrení potrebných pre implementáciu má organizačný, administratívny a manažérsky charakter (dá sa retalizovať po vytvorení potrebných kapacít – personálnych, kompetenčných, finančných, časových).

V kontexte riadenia KIB ide o dlhodobý proces správy rizík, ktorý zahŕňa aj aktivity, pri ktorých sa identifikujú nové riziká, ale aj sledovanie a prehodnocovanie existujúcich rizík, prijímanie opatrení a sledovanie ich účinnosti vrátane kontroly a auditu.

7 Prílohy

7.1 Identifikácia aktív

Aktívum je všetko, čo má pre organizáciu cenu, môže byť objektom pôsobenia hrozby a vyžaduje si ochranu. Pre danú úroveň podrobnosti sa aktívum považuje za elementárnu jednotku, ktorá sa už nedelí na menšie zložky.

Uvažujeme aktíva z definovanej oblasti, organizácie. Aktíva sa delia na primárne a podporné.

Primárne aktíva organizácie sú napr.:

- činnosti a aktivity organizácie
- informácia

Podporné aktíva sú tie, od ktorých závisia primárne aktíva, napr.:

- hardvér
- softvér
- sieť
- personál
- sídlo
- organizačná štruktúra

Zoznam aktív je súčasťou vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. ako **Príloha č. 1**.

7.1.1 Identifikácia primárnych aktív

Procesy, napr.:

- procesy, ktorých strata alebo narušenie znemožnia organizácii aby plnila svoje poslanie
- procesy spracúvajúce klasifikované alebo citlivé informácie
- procesy, ktorých modifikácia by podstatne skomplikovala plniť organizácii jej poslanie
- procesy, ktoré organizácia potrebuje na plnenie právnych, zmluvných a iných záväzných požiadaviek.

Informácia, napr.:

- informácia, bez ktorej organizácia nemôže plniť svoje poslanie
- osobné údaje
- strategické informácie, potrebné na dosiahnutie strategických cieľov organizácie
- informácia, ktorej zhromažďovanie, uchovávanie, spracovávanie a prenos trvalo dlhý čas a vyžaduje si veľké náklady

7.1.2 Identifikácia podporných aktív

Tieto aktíva podporujú primárne aktíva, majú zraniteľnosti, ktoré môžu využiť hrozby a narušením podporných aktív môžu narušiť primárne aktíva. Nižie je uvedené možné rozdelenie:

- Hardvér (všetky fyzické zariadenia, ktoré podporujú procesy spracovania informácie)
  - zariadenia na automatizované spracovanie údajov,
  - prenosné zariadenia (notebook, smartfón),
  - pevné zariadenia (servery a počítače používané v priestoroch organizácie, vrátane osobných počítačov),
  - periférne zariadenia pripojené k počítačom (tlačiareň).
- Pamäťové médiá
  - prenosné pamäťové médiá,
  - ostatné médiá na záznam informácie (papierová dokumentácia).
- Softvér (všetky programy, podieľajúce sa na spracovaní údajov)
  - operačný systém,
  - softvér slúžiaci na správu, diagnostiku a údržbu systémov, aplikácií, siete,
  - štandardný „krabicový“ softvér,
  - Štandardný aplikačný softvér (účtovný, administratívny, atď.),
  - Špeciálny aplikačný softvér (vyvinutý, alebo upravený pre potreby organizácie).
- Sieť (všetky telekomunikačné zariadenia slúžiace na prepojenie fyzicky vzdialených počítačov alebo prvkov informačného systému)
  - aktívne prvky,
  - komunikačné rozhrania.
- Personál (všetci ľudia s prístupom k informačným aktívam organizácie)
  - vedúci pracovníci,
  - používatelia,
  - informatici (správcovia, operátori, pracovníci help desk-u),
  - bezpečnostní manažéri,
  - vývojári.
- Sídlo
  - všetky fyzické priestory organizácie a fyzická infraštruktúra potrebná na ich prevádzku.
- Lokalita/poloha
  - externé prostredie (miesta, kde sa nedajú presadzovať bezpečnostné opatrenia organizácie, napr. verejné priestory, priestory inej organizácie, byty zamestnancov),
  - budovy na vlastných pozemkoch s fyzickým oddelením od ostatného sveta,

- zóna (vyčlenené priestory v budove),
- podstatné služby (všetky služby potrebné na to, aby zariadenia organizácie fungovali),
- komunikácia (internet, telekomunikačné služby a zariadenia poskytnuté operátorom),
- podporné služby – elektrina, voda, odvoz odpadu, klimatizácia.

- Organizácia
  - autority (nadriadené orgány, vedenie organizácie, entity, ktoré môžu rozhodovať, klásť podmienky a obmedzenia pre organizáciu),
  - štruktúra organizácie,
  - dodávatelia a poskytovatelia služieb.

7.2 Zoznam hrozieb

Zoznam hrozieb bol pripravený na základe hrozieb uvedených v medzinárodnom štandarde 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):

	Hrozba
H.1	Oheň
H.2	Voda
H.3	Znečistenie, škodlivé žiarenie
H.4	Veľká havária
H.5	Výbuch
H.6	Prach, korózia, zamrznutie
H.7	Klimatické javy
H.8	Seizmické javy
H.9	Vulkanické javy
H.10	Meteorologické javy
H.11	Povodeň
H.12	Pandémia / epidémia
H.13	Prerušenie zásobovacieho systému
H.14	Porucha chladiaceho alebo ventilačného systému
H.15	Výpadok napájania
H.16	Zlyhanie telekomunikačnej siete
H.17	Zlyhanie telekomunikačného zariadenia
H.18	Elektromagnetické žiarenie
H.19	Tepelné žiarenie
H.20	Elektromagnetické impulzy
H.21	Porucha zariadenia alebo systému
H.22	Zahltenie informačného systému
H.23	Porušenie udržiavateľnosti informačného systému
H.24	Teror, útok, sabotáž
H.25	Sociálne inžinierstvo
H.26	Nežiadúce elektronické vyžarovanie

Hrozba	
H.27	Špionáž
H.28	Odpočúvanie
H.29	Krádež médií alebo dokumentov
H.30	Krádež zariadenia
H.31	Krádež digitálnej identity alebo prihlasovacích údajov
H.32	Obnova recyklovaných alebo vyradených médií
H.33	Zverejňovanie informácií
H.34	Zadávanie údajov z nedôveryhodných zdrojov
H.35	Neoprávnená manipulácia s hardvérom
H.36	Neoprávnená manipulácia so softvérom
H.37	Drive-by útok
H.38	Opakovaný útok, útok typu man-in-the-middle
H.39	Neoprávnené spracúvanie osobných údajov
H.40	Neoprávnený vstup do objektov
H.41	Neoprávnené použitie zariadení
H.42	Nesprávne používanie zariadení
H.43	Poškodenie zariadení alebo médií
H.44	Podvodné kopírovanie softvéru
H.45	Používanie falšovaného alebo kopírovaného softvéru
H.46	Poškodzovanie údajov
H.47	Nezákonné spracovanie údajov
H.48	Odosielanie alebo distribúcia malvéru
H.49	Detekcia polohy
H.50	Chyba pri používaní
H.51	Zneužitie práv alebo povolení
H.52	Falšovanie práv alebo povolení
H.53	Zamietnutie konania
H.54	Nedostatok personálu
H.55	Nedostatok zdrojov
H.56	Zlyhanie poskytovateľov služieb
H.57	Porušenie zákonov alebo predpisov

7.3 Zoznam zraniteľností

V tejto časti je uvedený zoznam zraniteľností prevzatý najmä z medzinárodného štandardu 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). Pre každú zraniteľnosť sú na ilustráciu uvedené hrozby, ktoré môžu danú zraniteľnosť využiť.

P. č.	Kategória	Zraniteľnosť
Z.1	Zamestnanci	Nedostupnosť zamestnancov
Z.2		Neadekvátne postupy v procese prijímania zamestnancov
Z.3		Nedostatočné bezpečnostné školenia
Z.4		Nesprávne používanie softvéru a hardvéru
Z.5		Slabé povedomie o bezpečnosti
Z.6		Nedostatočné alebo chýbajúce monitorovacie nástroje
Z.7		Nedostatočné monitorovanie práce tretích strán
Z.8		Neúčinné alebo chýbajúce politiky správneho používania telekomunikačných médií a správ
Z.9	Lokalita	Nedostatočné vyžadovanie pravidiel fyzickej bezpečnosti pri vstupe do budov alebo miestností
Z.10		Poloha lokality v povodňovej oblasti
Z.11		Nestabilná elektrická sieť
Z.12		Nedostatočná fyzická ochrana budov, dverí a okien
Z.13	Organizácia	Formálny postup prideľovania a odoberania prístupov nebol implementovaný alebo jeho implementácia je neúčinná
Z.14		Formálny proces preskúmania prístupových práv nebol implementovaný alebo jeho vykonávanie je neúčinné
Z.15		Nedostatočné ustanovenia (týkajúce sa bezpečnosti) v zmluvách so zákazníkmi a/alebo tretími stranami
Z.16		Postupy monitorovania objektov na spracovanie informácií, neboli implementované alebo je ich implementácia neúčinná
Z.17		Bezpečnostné audity sa nevykonávajú pravidelne
Z.18		Postupy identifikácie a hodnotenia rizík neboli implementované alebo ich vykonávanie je neúčinné
Z.19		Nedostatočné alebo chýbajúce hlásenia o poruchách
Z.20		Nedostatočná reakcia servisnej údržby
Z.21		Nedostatočná alebo chýbajúca dohoda o úrovni poskytovaných služieb

Z.22	Organizácia	Postup kontroly implementovaných zmien nebol implementovaný alebo jeho implementácia je neúčinná
Z.23		Formálny postup pre kontrolu dokumentácie ISMS nebol implementovaný alebo jeho implementácia je neúčinná
Z.24		Formálny postup pre dohľad nad záznamami ISMS nebol implementovaný alebo jeho implementácia je neúčinná
Z.25		Formálny proces schvaľovania verejne dostupných informácií nebol implementovaný alebo implementácia je neúčinná
Z.26		Nesprávne rozdelenie zodpovedností za informačnú bezpečnosť
Z.27		Plány kontinuity neexistujú, sú neúplné alebo sú zastarané
Z.28		Pravidlá používania e-mailov neboli zavedené alebo ich implementácia je neúčinná
Z.29		Postupy zavádzania softvéru do operačných systémov neboli implementované alebo ich implementácia je neúčinná
Z.30		Postupy pre zaobchádzanie s utajovanými informáciami nie sú vyvinuté alebo ich vykonávanie je neúčinné
Z.31		Povinnosti v oblasti informačnej bezpečnosti nie sú uvedené v popisoch práce
Z.32		Nedostatočné alebo chýbajúce ustanovenia (týkajúce sa informačnej bezpečnosti) v zmluvách so zamestnancami
Z.33		Disciplinárne konanie v prípade incidentu v oblasti informačnej bezpečnosti nie je riadne zavedené
Z.34		Formálna politika používania prenosných počítačov nebola implementovaná alebo jej implementácia je neúčinná
Z.35		Nedostatočná kontrola informačných aktív, ktoré sa nachádzajú mimo primárnej lokality
Z.36		Nedostatočná alebo chýbajúca politika "čistého stola a čistej obrazovky"
Z.37		Autorizácia objektov na spracovanie informácií nie je implementovaná alebo nefunguje správne
Z.38		Mechanizmy monitorovania narušenia bezpečnosti neboli riadne implementované
Z.39		Postupy na hlásenie nedostatkov v oblasti bezpečnosti neboli vyvinuté alebo ich implementácia je neúčinná
Z.40		Postupy súladu, ktoré sa týkajú duševného vlastníctva, neboli vypracované alebo ich vykonávanie je neúčinné

7.4 Bezpečnostné opatrenia definované Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ďalšie informácie o bezpečnostných opatreniachako riešeniach, ktorých zavedením (implementáciou) sa eliminuje alebo aspoň zníži úroveň rizika, je v prípade potreby hlbšieho prieniku do problematiky možné získať aj štúdiom medzinárodných noriem, zaoberajúcich sa oblasťou KIB. Jednou z nich je metodika BSI, v rámci ktorej je možné bezpečnostné opatrenia rozdeliť podľa používaných prostriedkov na:

a) technické,

b) organizačné a

c) prevádzkové.

Technické opatrenia sú založené na bezpečnostných funkciách realizovaných pomocou hardvérových komponentov, firmvéru a softvéru.

Organizačné opatrenia sa realizujú pomocou politík, pravidiel, záväzných postupov, stanovení zodpovednosti, školení zamestnancov, zmlúv.

Prevádzkové opatrenia zahŕňajú fyzickú ochranu IKT, podpornej infraštruktúry, ochranu prístupu, detekcie pohybu, detekcie požiaru a pod.

Podľa toho, na ktorú fázu potenciálneho bezpečnostného incidentu spôsobeného naplnením hrozby pôsobia, je možné rozdeliť na:

a) preventívne,

b) detekčné,

c) korekčné.

Úlohou **preventívnych opatrení** je zamedziť vzniku bezpečnostného incidentu, alebo aspoň výrazne znížiť pravdepodobnosť naplnenia hrozby. Preventívne opatrenia sú zamerané buď na odstránenie zraniteľnosti, ktorú hrozba využíva, alebo v prípade, ak je nositeľom hrozby človek, na zníženie jeho útočného potenciálu (motivácie: napr. zvýšenie pravdepodobnosti jeho odhalenia a potrestania – odstrašenie,príležitosť: na prekonanie nových opatrení potrebuje podstatne väčšie zdroje,znalosti: odstránenie známych zraniteľností, ktoré umožňovali útoky).

Detekčné opatrenia predstavujú druhú úroveň ochrany aktív. Ich cieľom je odhaliť včas začínajúci bezpečnostný incident, signalizovať ho napr. operátorovi a zaznamenať údaje potrebné na analýzu vzniku a priebehu bezpečnostného incidentu. Príkladmi detekčných opatrení sú zariadenia na detekciu pohybu, dymu, IDS (intrusion detection systems, systémy na detekciu prieniku), monitorovacie programy, systémy na vytváranie záznamov auditu a pod.

Korekčné opatrenia sú zamerané na zabezpečenie kontinuity činnosti: v prípade bezpečnostných incidentov na ich riešenie a na návrat aktíva do normálneho stavu.

Posledným krokom pred výberom opatrení na ošetrenie neakceptovateľných rizík je analýza ekonomickej efektívnosti (cost/benefit) navrhovaných opatrení, ktorú pripravuje pracovná skupina. Vstupom pre analýzu ekonomickej efektívnosti je zoznam identifikovaných rizík. Ku každému riziku sú priradené možné opatrenia a analýza pozostáva z:

- určenia dopadu zavedenia nového alebo rozšírenia existujúceho opatrenia,

- určenia dopadu toho, že sa nové opatrenie nezavedie alebo existujúce opatrenie nerozšíri,
- odhadu nákladov na zavedenie nového alebo rozšírenia existujúceho opatrenia, napr.:
  - kúpa technických zariadení a/alebo softvéru,
  - prípadné zníženie efektívnosti činnosti systému v dôsledku zavedenia opatrenia,
  - náklady spojené so zavedením dodatočných politík a procedúr,
  - náklady na personál potrebný na zavedenie nových opatrení (pracovný čas existujúcich zamestnancov, alebo prostriedky spojené s prijatím nových zamestnancov)
  - náklady na školenia zamestnancov,
  - náklady na údržbu,
- porovnanie nákladov na zavedenie nového alebo rozšírenia existujúceho opatrenia a jeho prínosu vzhľadom na význam tých systémov a údajov pre organizáciu, ktorých ochrana sa daným opatrením zvýši (resp. u ktorých sa zníži úroveň rizika).

Záverečné rozhodnutie je na vedúcom zamestnancovi (alebo vedení) organizácie, ktorý musí posúdiť, či je v danom prípade riziko akceptovateľné alebo nie, a či návrh na zavedenie nového opatrenia možno zamietnuť alebo nie. Pre rozhodovanie o zavedení nového opatrenia môžu pomôcť nasledujúce pravidlá:

- ak opatrenie redukuje riziko viac, než je potrebné, treba sa pozrieť, či neexistuje iné, lacnejšie riešenie,
- ak je cena navrhovaného riešenia ako hodnota, o ktorú redukuje riziko, treba hľadať iné riešenie
- ako opatrenie neredukuje riziko dostatočne, treba sa pozrieť na ďalšie doplňujúce opatrenia alebo nejaké iné opatrenie,
- ak navrhované opatrenie redukuje riziko dostatočne a je spomedzi možných opatrení najlacnejšie, treba ho použiť.

7.5 Bezpečnostné opatrenia definované National Institute of Standards and Technology (NIST)

Ďalšie informácie o bezpečnostných opatreniachako riešeniach, ktorých zavedením (implementáciou) sa eliminuje alebo aspoň zníži úroveň rizika, je v prípade potreby hlbšieho prieniku do problematiky možné získať aj štúdiom medzinárodných noriem, zaoberajúcich sa oblasťou KIB. Ďalšou z nich je metodika **NIST Special publication SP 800 53 r5**, podľa ktorejmá organizácia zaviesť nasledovné bezpečnostné opatrenia:

Riadenie prístupu (Access Control - AC)

Organizácia musí zabezpečiť:

- aby prístup k systému mali len oprávnené osoby a iné zariadenia alebo systémy (externé počítače),
- aby oprávnené osoby mohli pristupovať (priamo, alebo prostredníctvom iných systémov alebo procesov) len k tým zdrojom systému, na ktoré majú oprávnenia a vykonávať len tie činnosti, na ktoré sú oprávnené.

Bezpečnostné povedomie a tréning (Awareness and Training - AT)

Organizácia musí zabezpečiť:

- aby si manažéri a používatelia IKT systémov v organizácii boli vedomí a bezpečnostných rizík spojených s ich činnosťou a požiadaviek, ktoré pre nich vyplývajú v tejto súvislosti z príslušných zákonov, bezpečnostnej politiky a ďalšej vnútornej legislatívy organizácie, bezpečnostných štandardov a prevádzkového poriadku IKT systémov;
- aby bol personál a používatelia primerane trénovaní na to, aby si dokázali plniť povinnosti podľa prvého bodu týkajúce sa bezpečnosti prevádzky a používania IKT systémov.

Audit a dosledovateľnosť (Audit and Accountability AU)

Organizácia musí:

- vytvárať, chrániť a udržiavať záznamy auditu činnosti IKT systému v rozsahu potrebnom na to, aby bolo možné monitorovať, analyzovať, vyšetrovať a nahlasovať protizákonné, neoprávnené alebo neprimerané aktivity v IKT systéme,
- zabezpečiť, aby jednotlivé aktivity v IKT systéme boli jednoznačne spojené s používateľmi, ktorí ich vykonali a tak títo používatelia mohli byť braní na zodpovednosť za svoju činnosť v systéme.

Certifikácia, akreditácia a bezpečnostné ohodnotenie (Certification, Accreditation, and Security Assessments - CA)

Organizácia musí:

- periodicky vyhodnocovať bezpečnostné opatrenia v IKT systémoch organizácie, aby určila, či sú opatrenia účinné,
- vypracovať a implementovať plány činnosti zamerané na opravu nedostatkov a redukciu alebo odstránenie zraniteľností v IKT systémoch organizácie,
- povoliť prevádzku IKT systémov organizácie a pripojenie externých systémov k nim,

- neustále monitorovať bezpečnostné opatrenia na ochranu IKT systémov, aby zaistila ich stálu účinnosť

Manažment konfigurácie (Configuration Management - CM)

Organizácia musí:

- zaviesť a udržiavať základné konfigurácie IKT systémov a katalógy IKT systémov (hw, sw, firmware a dokumentácia) organizácie počas ich životných cyklov
- zaviesť a presadzovať nastavenia bezpečnostnej konfigurácie IKT produktov používaných v IKT systémoch organizácie

Havarijné plánovanie (Contingency Planning (CP)

Organizácia musí:

- vypracovať, udržiavať a efektívne implementovať plány reakcie v mimoriadnych situáciách, zálohovacie procedúry a plány obnovy pre IKT systémy organizácie, aby zaistila dostupnosť kritických informačných zdrojov a kontinuitu operácií v mimoriadnych situáciách

Identifikácia a autentifikácia (Identification and Authentication - IA)

Organizácia musí:

- identifikovať používateľov IKT systémov, zariadení, procesov konajúcich v záujme používateľov; a overiť identity týchto používateľov, procesov alebo zariadení ešte pred tým ako im povolí prístup k IKT systémom organizácie

Reakcia na incidenty (Incident Response - IR)

Organizácia musí:

- pre IKT systémy organizácie vytvoriť operačné kapacity na riešenie bezpečnostných incidentov, ktoré sú schopné vykonávať adekvátnu prípravu zamestnancov, detekciu, analýzu, ohraničenie bezpečnostného incidentu, obnovu IKT systému po incidente a primerané reakcie používateľov na incident,
- vystopovať, zdokumentovať a nahlasovať príslušným riadiacim pracovníkom organizácie, prípadne úradom.

Údržba (Maintenance - MA)

Organizácia musí:

- vykonávať aktuálnu (podľa potreby) a periodickú údržbu IKT systémov organizácie,
- zabezpečovať efektívny dohľad nad nástrojmi, technikami, mechanizmami, ktoré sa používajú pri údržbe a personálom ktorý údržbu vykonáva.

Ochrana médií (Media Protection - MP)

Organizácia musí:

- chrániť pamäťové média tak papierové ako aj digitálne (elektronické),
- omedziť prístup k informáciám uloženým na pamäťových médiách IKT systému len pre oprávnené osoby,

- zničiť pamäťové médiá pred ich vyradením alebo bezpečne odstrániť údaje z pamäťových médií pred ich opätovným použitím.

Fyzická ochrana a ochrana prostredia (Physical and Environmental Protection - PE)

Organizácia musí:

- obmedziť fyzický prístup k IKT systémom, zariadeniam a do ich operačného prostredia len na oprávnené osoby
- chrániť fyzické zariadenia a podporovať infraštruktúru IKT systémov
- poskytovať pre IKT systémy podporné zariadenia potrebné pre ich prevádzku
- chrániť IKT systémy proti prírodným hrozbám a hrozbám z prostredia
- zaistiť primerané environmentálne opatrenia v zariadeniach v ktorých sú umiestnené IKT systémy

Plánovanie (Planning - PL)

Organizácia musí:

- vyvinúť, zdokumentovať, periodicky aktualizovať a implementovať bezpečnostné plány pre IKT systémy organizácie, ktoré popisujú použité alebo plánované bezpečnostné opatrenia pre IKT systémy a pravidlá správania jednotlivcov, pristupujúcich k IKT systémom.

Personálna bezpečnosť (Personnel Security - PS)

Organizácia musí:

- zabezpečiť, aby jednotlivci ktorí zastávajú zodpovedné funkcie v organizácii (vrátane tretích strán poskytujúcich služby organizácii) boli dôveryhodné osoby a spĺňali bezpečnostné kritériá stanovené pre dané funkcie, zaistiť, aby informácie a IKT systémy organizácie boli chránené počas personálnych zmien a po nich, ako sú ukončenie pracovného pomeru alebo zmena pracovného zaradenia,
- zaviesť a uplatňovať formálne sankcie voči zamestnancom, ktorí konali v rozpore s bezpečnostnou politikou alebo bezpečnostnými procedúrami organizácie.

Ohodnotenie rizík (Risk Assessment - RA)

Organizácia musí:

- periodicky ohodnocovať riziká voči aktivitám organizácie (vrátane poslania organizácie, funkcií, ktoré plní, imidžu alebo reputácie), aktívam organizácie, a jednotlivcom, ktoré vyplývajú z činnosti IKT systémov organizácie a s nimi súvisiaceho spracovania, uchovávania alebo prenosu informácie.

Obstarávanie systémov a služieb (System and Services Acquisition - SA)

Organizácia musí:

- vyhradiť dostatočné zdroje na primeranú ochranu IKT systémov organizácie
- používať v priebehu celého životného cyklu systému také procesy, ktoré zohľadňujú bezpečnostné aspekty systému
- dodržiavať obmedzenia na inštaláciu a používanie softvéru

- zaistiť, aby tretie strany pri poskytovaní služieb organizácii používali adekvátne bezpečnostné opatrenia na ochranu informácie, aplikácií a/alebo služieb ktoré organizácii poskytujú

Ochrana systému a komunikácie (System and Communications Protection - SC)

Organizácia musí:

- monitorovať, kontrolovať a chrániť komunikáciu organizácie (t.j. informácie vysielanú alebo prijímanú IKT systémami organizácie) na vonkajších hraniciach a kľúčových vnútorných hraniciach informačných systémov
- uplatňovať pri vývoji a prevádzke IKT systémov také návrhy architektúry, techniky vývoja softvéru ainžinierske princípy, ktoré podporujú informačnú bezpečnosť v IKT systémoch organizácie.

Integrita systému a informácie (System and Information Integrity - SI)

Organizácia musí:

- včas identifikovať, nahlasovať a korigovať chyby v informácii a v IKT systémoch organizácie,
- na vhodnom mieste IKT infraštruktúry organizácie (centrálne a/alebo distribuovane) zabezpečovať ochranu IKT systémov pred škodlivým softvérom
- monitorovať bezpečnostné výstrahy a odporúčania systému a primerane na ne reagovať.

7.6 Návrh štruktúry konkrétneho dokumentu bezpečnostného projektu

Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.1 | kyberbezpecnost@mirri.gov.sk | december 2022

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Návrh štruktúry konkrétneho dokumentu bezpečnostného projektu

Obsah

I. Základné identifikačné údaje dokumentu

II. Zmenový list

Verzia	
Gestor	
Dátum poslednej revízie	
Dátum vydania	
Dátum účinnosti	

III. Súvisiace dokumenty

IV. Použitá terminológia a skratky

V. Zoznam právnych predpisov

Zoznam právnych predpisov aplikovaných v bezpečnostnom projekte:

- smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii – smernica NIS,
- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „zákon o kybernetickej bezpečnosti“),
- vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
- vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
- vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
- zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) – GDPR,
- zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- autorský zákon č. 185/2015 Z. z. v znení neskorších predpisov.
- 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 (NBÚ)

VI. Účel bezpečnostného projektu IS

Bezpečnostný projekt IS definuje formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov organizácie, technických noriem a štandardov dobrej praxe. Dokument obsahuje komplexné posúdenie bezpečnostných potrieb, určenie bezpečnostných požiadaviek, návrh spôsobu ich efektívneho naplnenia a vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika.

Bezpečnostný projekt slúži na eliminovanie a minimalizovanie rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti. Správca tohto informačného systému chráni spracúvané informácie pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania.

Pri každom riziku sa zohľadňuje pravdepodobnosť situácie, pri ktorej hrozby využijú existujúce zraniteľnosti a spôsobia negatívny vplyv na aktíva orgánu riadenia. Pri hodnotení závažnosti výsledného vplyvu sa zohľadňuje celková závažnosť vplyvov, ktoré môžu byť spôsobené pri realizácii rizika. Úroveň vplyvov sa určuje osobitne pre každé analyzované riziko a zahŕňa všetky aktíva dotknuté príslušným rizikom. Analyzované riziko môže mať na aktíva orgánu riadenia viaceré vplyvy, ktoré je potrebné sumárne vyhodnotiť a zdokumentovať. Výsledná miera rizika musí zohľadňovať aj všetky realizované bezpečnostné opatrenia.

Na tento účel sú prijímané primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracúvania informácií, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných informácií, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému. Prijatím bezpečnostných opatrení správca neoprávneným osobám znemožňuje akýkoľvek nedovolený prístup k spracúvaným informáciám a oprávneným osobám zabezpečí prístup k informáciám v rozsahu potrebnom na plnenie ich povinností.

VII. Ciele bezpečnostného projektu IS

Hlavnými strategickými bezpečnostnými cieľmi z pohľadu kybernetickej bezpečnosti sú:

- Informačná a kybernetická bezpečnosť ako základná súčasť DNA organizácie
- Dôveryhodná organizácia pripravená na hrozby
- Riadiť kybernetickú a informačnú bezpečnosť v súlade s požiadavkami platnej legislatívy SR aj EÚ, medzinárodnými štandardmi a odporúčaniami odvetvovej praxe
- Zabezpečovať primeranými technickými, organizačnými a personálnymi bezpečnostnými opatreniami ochranu dôvernosti, integrity a dostupnosti informačných aktív
- Zabezpečovať primeranými technickými, organizačnými a personálnymi opatreniami ochranu informácií v informačných systémoch, vrátanie osobných údajov pred odcudzením, nedostupnosťou, poškodením, neoprávneným prístupom, zmenou a rozširovaním
- Implementovať a udržiavať plán reakcie na kybernetické bezpečnostné incidenty
- Podieľať sa na zaistení kontinuity činností spoločnosti v prípade kybernetických bezpečnostných incidentov
- Zvyšovať povedomie o kybernetickej a informačnej bezpečnosti všetkých zamestnancov a vedenia inšitúcie
- Riadiť riziká kybernetickej a informačnej bezpečnosti s cieľom implementovať efektívne opatrenia na ich minimalizáciu
- Zaistiť bezpečnú prevádzku a správu informačných systémov
- Zabezpečiť dôvernosť, dostupnosť a integritu najmä osobných údajov, obchodného tajomstva a iných dôležitých informačných aktív organizácie, fyzických a právnických osôb pri ich spracúvaní
- Minimalizácia finančných a iných strát súvisiacich s narušením prevádzky informačných systémov
- Zaistenie poskytovania služieb informačného systému užívateľom informačného systému v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch informačného systému
- Ochrana dobrého mena organizácie

VIII. Bezpečnostný zámer (základné bezpečnostné ciele)

IX. Analýza bezpečnosti

Táto podkapitola obsahuje zoznam existujúcich a navrhovaných opatrení pre všetky oblasti bezpečnosti definované v rámci zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Ide o nasledujúce oblasti:

a) organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
b) riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
c) personálna bezpečnosti,
d) riadenie prístupov,
e) riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
f) bezpečnosť pri prevádzke informačných systémov a sietí,
g) hodnotenie zraniteľností a bezpečnostných aktualizácií,
h) ochrana proti škodlivému kódu,
i) sieťová a komunikačná bezpečnosť,
j) akvizícia, vývoj a údržba informačných sietí a informačných systémov,
k) zaznamenávanie udalostí a monitorovanie,
l) fyzická bezpečnosť a bezpečnosť prostredia,
m) riešenie kybernetických bezpečnostných incidentov,
n) kryptografické opatrenia,
o) kontinuita prevádzky,
p) audit, riadenie súladu a kontrolných činností.

X. Navrhované bezpečnostné opatrenia

XI. Určenie nepokrytých rizík

XII. Vymedzenie kritérií na akceptáciu rizika

XIII. Ohraničenia aktíva, pre ktoré je analýza rizík spracovaná

XIV. Postupy revízie analýzy rizík