MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Metodika analýzy bezpečnosti pre bezpečnostné projekty ISVS

Obsah

1. Správa dokumentu

Tento dokument je metodickým materiálom slúžiacim pre potreby orgánov verejnej moci. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie. Nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

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

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.

2. Úvod

Účelom tohto dokumentu je metodicky upraviť výkon kvalitatívnej analýzy rizík ako súčasti analýzy bezpečnosti v rámci bezpečnostného projektu ISVS.

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. Cieľom analýzy rizík má byť identifikácia okolností, ktoré potenciálne môžu narušiť bezpečnosť ISVS (t. j. zraniteľností, hrozieb, scenárov rizík). Základnou zásadou tejto metodiky je všeobecná použiteľnosť v prostredí verejnej správy.

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).

Pre riziká týkajúce sa okolia, na ktoré v rámci bezpečnostného projektu konkrétneho ISVS nie je dosah, musia byť bezpečnostné opatrenia popísané formou požiadaviek, resp. odporúčaní na okolie.

Táto metodika sa opiera najmä o nasledovné právne predpisy:

- Zákon č. 95/2019 Z. z. informačných technológiách vo verejnej správe,
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti,
- Vyhláška UPVII č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- Vyhláška NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Analýza rizík vykonaná podľa tejto metodiky spĺňa požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a zákona č. 95/2019 Z. z. informačných technológiách vo verejnej správe.

Pokiaľ nie je uvedená verzia referencovaného 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 (najmä 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. Štruktúra bezpečnostného projektu ISVS

V tejto kapitole sú popísané základné okruhy informácií tvoriace bezpečnostný projekt ISVS, ich rozdelenie do jednotlivých dokumentov a metodický postup vypracovania bezpečnostného projektu.

Bezpečnostný projekt ISVS je tvorený dvoma hlavnými výstupmi:

- bezpečnostný zámer,
- analýza bezpečnosti (zahŕňa analýzu rizík).

Tieto dokumenty musia byť vytvárané aj v súlade so stanoveným časovým harmonogramom podľa vyhlášky MIRRI č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy (v prípade, že sa táto vzťahuje na projekt vývoja/rozvoja ISVS).

Obsah a štruktúra bezpečnostného projektu informačného systému verejnej správy a jeho výstupov vychádza z prílohy č. 3 vyhlášky UPVII č. 179/2020 Z. z..

Štruktúra výstupu analýzy bezpečnosti musí zodpovedať oblastiam ustanoveným osobitným predpisom[1] alebo technickou normou.[2] Finalizácia dokumentácie bezpečnostného projektu informačného systému verejnej správy je realizovaná v etape IMPLEMENTÁCIA A TESTOVANIE v súlade s vyhláškou Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy.

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

3.1. Tvorba bezpečnostného zámeru

Ako prvý výstup bezpečnostného projektu ISVS sa vypracuje dokument bezpečnostný zámer. Bezpečnostný zámer určuje najmä kontext a zameranie bezpečnostného projektu, preto obsahuje najmenej:

a) formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov orgánu riadenia, technických noriem a štandardov dobrej praxe,
b) zoznam právnych predpisov aplikovaných v bezpečnostnom projekte, ako aj interných riadiacich aktov,
c) metodický prístup ku kvalitatívnej analýze rizík, ktorá je v bezpečnostnom projekte vykonaná,
d) 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,

[1] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

[2] napríklad STN EN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti

e) 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,
f) vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,
g) ohraničenia bezpečnostného projektu (explicitné vysvetlenie oblastí, ktoré bezpečnostný projekt nezahŕňa alebo kladie požiadavky na ich riešenie mimo projektu informačného systému verejnej správy),
h) postupy revízie/aktualizácie bezpečnostného zámeru.

3.2. Tvorba analýzy bezpečnosti

Hlavným výstupom bezpečnostného projektu informačného systému verejnej správy je dokument analýzy bezpečnosti, ktorého súčasťou je kvalitatívna analýza rizík. Rizikom sa v bezpečnostnom projekte chápe miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho následkami. 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 a priamo nadväzuje na dokument bezpečnostný zámer.

Analýza rizík pozostáva najmä z výkonu nasledovných činností:
a) vytvorenie podkladových katalógov pre analyzované riziká určených na identifikáciu aktív, identifikáciu hrozieb a zraniteľností a identifikáciu následkov[3],
b) identifikácia a opis analyzovaných scenárov rizík,
c) priradenie aktív, hrozieb, zraniteľností a vplyvov ku každému z identifikovaných scenárov rizík,
d) identifikácia realizovaných (existujúcich) bezpečnostných opatrení,
e) vyhodnotenie scenárov rizík spôsobom kombinácie pravdepodobnosti realizácie scenáru rizika a závažnosti následku,
f) formulácia navrhovaných bezpečnostných opatrení.

Obsahová štruktúra výstupu analýzy bezpečnosti musí pokrývať minimálne nasledovné oblasti:

a) organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,
b) správu zraniteľností a kybernetických hrozieb,
c) správu aktív a riadenie kybernetických hrozieb a rizík,
d) riadenie udalostí a kybernetických bezpečnostných incidentov,
e) riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie,
f) bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií,
g) postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,
h) kryptografické opatrenia a zásady používania kryptografie,

[3] historicky označované aj ako dopady

i) bezpečnosť a spôsobilosti ľudských zdrojov,
j) správu identít a prístupov,
k) bezpečnosť pri prevádzke sietí a informačných systémov,
l) ochranu proti škodlivému kódu a nežiaducemu obsahu,
m) systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,
n) monitorovanie, zaznamenávanie a hlásenie udalostí,
o) fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení,
p) ochranu záznamov, súkromia a označovanie informácií,
q) dodávateľský reťazec,
r) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT.

V prípade, že analyzovaný ISVS spracúva osobné údaje, môže byť identifikovaná potreba vykonania posúdenia vplyvu na ochranu osobných údajov. Konkrétne špecifiká a podrobnosti o spracúvaní osobných údajov a z toho vyplývajúcich povinností z nariadenia GDPR musia byť uvedené v posúdení vplyvu na ochranu osobných údajov (DPIA - Data Protection Impact Assessment), ktoré však nie je súčasťou bezpečnostného projektu IS. Jeho vypracovanie, resp. aktualizácia, je v zodpovednosti prevádzkovateľa IS (v zmysle GDPR).

4. Metodika analýzy rizík

Analýza rizík ISVS má byť založená na kvalitatívnej metodike analýzy rizík a realizovaná na základe požiadaviek vyhlášky UPVII č. 179/2020, ako aj ďalších bezpečnostných štandardov. Ako zdroj tejto metodiky pre analýzu rizík IS boli použité najmä:

- kvalitatívna metodika analýzy rizík vydaná NBÚ s názvom Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti,
- ENISA Interoperable EU Risk Management Framework, ENISA interoperable EU Risk Management Toolbox, December 2022,
- STN ISO/IEC 27005:2023 Informačná bezpečnosť, kybernetickábezpečnosť a ochrana súkromia – Usmernenie k riadeniu rizík informačnej bezpečnosti,
- NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments a NIST Special Publication 800-39 Managing Information Security Risk.

Analýza rizík IS slúži k podrobnému rozboru stavu kybernetickej a informačnej bezpečnosti. Cieľom analýzy rizík IS je identifikácia okolností, ktoré potenciálne môžu narušiť bezpečnosť ISVS a jeho okolia (t. j. hrozieb, zraniteľností, scenárov rizík).

Analýzou rizík sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcich zraniteľností aktív potenciálnymi hrozbami v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou následkov pri narušení dôvernosti, integrity alebo dostupnosti aktív.

4.1. Štruktúra, zameranie a kroky analýzy bezpečnosti ISVS

Analýza rizík ISVS slúži na identifikáciu rizík pôsobiacich na jednotlivé aktíva ISVS, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť systému. Jej výsledkom je spolu so zoznamom scenárov rizík (ktoré môžu ohroziť dôvernosť, integritu a dostupnosť dotknutých aktív) aj návrh bezpečnostných opatrení, ktoré sú schopné tieto riziká znížiť na akceptovateľnú úroveň.

Analýza rizík ISVS musí byť zameraná nasledovne:

- je vykonaná v súlade so zákonom o KB a zákonom o ITVS,
- cieľom je preskúmať úroveň bezpečnosti ISVS a identifikovať okolnosti, ktoré môžu bezpečnosť narušiť (riziká, resp. scenáre rizík),
- výsledkom analýzy rizík ISVS je ohodnotený zoznam identifikovaných scenárov rizík a návrh bezpečnostných opatrení, ktoré slúžia na ich ošetrenie,
- odhad pravdepodobnosti realizácie scenára rizika je vykonaný kvalitatívnou formou,
- vyhodnotenie závažnosti následkov pri realizácii scenára rizika je vyjadrené kvalitatívnou formou tak, aby bolo možné následne jednoznačne vyhodnotiť výslednú hodnotu rizika,
- vyhodnotenie výsledného zostatkového rizika je realizované ako kombinácia odhadu pravdepodobnosti realizácie scenára rizika a závažnosti z neho plynúcich následkov, po zohľadnení existujúcich bezpečnostných opatrení,
- identifikované hrozby, zraniteľnosti a zistené nedostatky súvisiace so scenárom sú sumarizované do konkrétnych scenárov rizík, v kontexte príslušných aktív,

- podrobná dokumentácia všetkých atribútov scenárov rizík je súčasťou výstupu analýzy bezpečnosti ISVS alebo osobitného dokumentu, ktorý je prílohou analýzy bezpečnosti ISVS (napr. v prípade, že sa na sumarizačnú dokumentáciu atribútov použije MS Excel),
- preferovanou metódou ošetrovania rizika je 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 scenár rizika akceptovateľný (t. j. či hodnota zvyškového rizika je na prijateľnej úrovni),
- konkretizácia rizík považovaných za akceptovateľné zostatkové riziká je stanovená na základe vymedzenia kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika stanovených v bezpečnostnom zámere, resp. v rámci procesov riadenia rizík,
- pre riziká týkajúce sa okolia, na ktoré v rámci analýzy rizík ISVS nie je dosah, sú bezpečnostné opatrenia popísané formou požiadaviek, resp. odporúčaní na okolie,
- analýza rizík ISVS musí byť vykonaná s podrobnosťou umožňujúcou (pri zohľadnení súčasných poznatkov o informačnej a kybernetickej bezpečnosti) považovať všetky riziká v nej neuvedené za akceptovateľné riziká.

Analýza bezpečnosti ISVS pozostáva z nasledujúcich krokov:

1. Stanovenie kontextu rizík
   - identifikácia aktív,
   - identifikácia potenciálnych hrozieb,
   - identifikácia zraniteľností,
   - identifikácia následkov,
   - identifikácia existujúcich opatrení,
   - identifikácia scenárov rizík.
2. Vyhodnotenie výsledných rizík
   - určenie pravdepodobnosti naplnenia scenárov rizík,
   - ohodnotenie následkov,
   - určenie úrovne výsledných rizík.
3. Návrh bezpečnostných opatrení

4.2. Stanovenie kontextu rizík

V tejto fáze analýzy rizík IS sú identifikované všetky podkladové materiály pre fázu identifikácie výsledného rizika, t. j. katalóg aktív, katalóg hrozieb, katalóg zraniteľností a prípadne aj katalóg následkov (vzory sú uvedené v prílohách). Súčasťou tejto fázy je aj identifikácia existujúcich opatrení pre všetky analyzované oblasti bezpečnosti IS a súvisiace scenáre rizík, a to vždy v úvodnej časti každej popisovanej oblasti bezpečnosti.

4.2.1. Identifikácia aktív

Základnou úlohou každej organizácie je ochrana svojich aktív. Aktíva sú hmotné, alebo nehmotné entity, ktoré pre organizáciu priamo, alebo nepriamo predstavujú súčasnú, alebo potenciálnu hodnotu. Aktíva sa môžu deliť na primárne (procesy/služby, informácie) a podporné (ľudské zdroje, hardvér, softvér, technologické komponenty, objekty a priestory organizácie, tretie strany).

Prvým krokom pri ochrane aktív súvisiacich s IS je vytvorenie ich prehľadného zoznamu, ktorý je jedným z hlavných vstupov do analýzy rizík. Katalóg aktív je vytvorený v rámci bezpečnostného projektu IS za účelom identifikácie a vyhodnotenia scenárov rizík v súlade so stanovenou metodikou. Môže byť aj podkladom pre komplexnú identifikáciu a evidenciu aktív podľa postupov definovaných v prostredí prevádzkovateľa ISVS.

Každému aktívu uvedenému v katalógu aktív IS musí mať prevádzkovateľ ISVS priradeného jeho vlastníka, ktorý je zodpovedný za správu a bezpečnosť daného aktíva v širšom kontexte riadenia aktív.[4] Vlastník aktíva sa určuje nielen na základe jeho vlastníckych práv, ale napr. aj na základe jeho zodpovednosti za tvorbu, vývoj, údržbu, prevádzku, prípadne bezpečnosť daného aktíva. V prípade, že prevádzkovateľ má v rámci riadenia rizík implementované procesy kvalitatívneho hodnotenia aktív a aktíva zahrnuté v analýze rizík IS už sú takto ohodnotené, je možné zahrnúť hodnoty aktív do identifikácie výsledného rizika, a to implicitne v rámci ohodnotenia príslušných negatívnych následkov podľa kap. 4.3.2.

Vzor katalógu aktív IS je uvedený v prílohe č. 1. V rámci výkonu analýzy rizík ISVS sú vždy skúmané len aktíva, ktoré majú priamy súvis s daným scenárom rizika. Pre jednotlivé scenáre rizík sú tak identifikované dotknuté aktíva, ich priradenie k scenárom rizík (uvedením zoznamu identifikátorov príslušných aktív) je zväčša súčasťou osobitného dokumentu, ktorý má byť prílohou analýzy bezpečnosti ISVS.

4.2.2. Identifikácia hrozieb

Hrozbou sa rozumie akákoľvek okolnosť či udalosť, ktorá môže potenciálne využiť zraniteľné miesto aktív a spôsobiť negatívny následok.

Z charakteru hrozieb vyplýva, že sú pre organizáciu potenciálnym ohrozením, prostredníctvom ktorého môže dôjsť k bezpečnostnému incidentu a významným negatívnym následkom na IS. Hrozba má vo všeobecnosti potenciál poškodenia aktív ISVS, môže byť prirodzeného alebo ľudského pôvodu, náhodná alebo úmyselná, môže vzniknúť z vnútorného ako aj vonkajšieho prostredia organizácie.

Pre efektívne riadenie rizík je nevyhnutné identifikovať všetky hrozby spôsobilé narušiť informačnú a kybernetickú bezpečnosť IS. V rámci identifikácie hrozieb pôsobiacich na ISVS musí byť vytvorený prehľadný zoznam (katalóg) hrozieb uvažovaných vo vzťahu k identifikovaným aktívam.

Vzor katalógu uvažovaných hrozieb je uvedený v prílohe č. 2. Je vytvorený na základe verejného katalógu hrozieb podľa Národného bezpečnostného úradu SR. Pôvod hrozieb je uvádzaný v zmysle požiadavky § 6 ods. 10 vyhlášky NBÚ č. 362/2018 (D – úmyselná, A – náhodná, E – vplyv prostredia).[5]

V rámci výkonu analýzy rizík ISVS sú vždy posudzované len hrozby, ktoré majú priamy súvis s daným scenárom rizika. Pre jednotlivé scenáre rizík sú tak identifikované hrozby, ktoré sú zdrojom daného rizika, ich priradenie k scenárom rizík (uvedením zoznamu

[4] v praxi nie je vlastníctvo aktív často jednoznačne určené, to však nepredstavuje prekážku pre ďalší výkon analýzy rizík ISVS. Vlastníctvo je však nutné doriešiť v súvisiacich procesoch riadenia rizík

[5] z angl. prekladu Deliberate, Accidental, Environmental

identifikátorov príslušných hrozieb) je zväčša súčasťou osobitného dokumentu, ktorý má byť prílohou analýzy bezpečnosti ISVS.

4.2.3. Identifikácia zraniteľností

Zraniteľnosť je takým miestom v prostredí IS resp. organizácie, ktoré má potenciál byť zneužité hrozbou a spôsobiť negatívny následok na aktíva organizácie, alebo organizáciu ako celok. Existencia zraniteľnosti nespôsobuje sama o sebe škodu, pretože musí existovať hrozba, ktorá ju využije. Zraniteľnosť, ktorá nemá zodpovedajúcu hrozbu, nemusí vyžadovať realizáciu opatrenia, ale mala by byť identifikovaná a sledovaná.

Vzor katalógu uvažovaných zraniteľností je uvedený v prílohe č. 3. Je vytvorený na základe štandardu STN ISO/IEC 27005:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia – Usmernenie k riadeniu rizík informačnej bezpečnosti.

V rámci analýzy rizík ISVS sú identifikované aj špecifické zraniteľnosti, ktoré môžu byť využité hrozbami na spôsobenie škody na identifikovaných aktívach. Ich zdokumentovanie vo vzťahu ku konkrétnym scenárom rizík (uvedením zoznamu identifikátorov príslušných zraniteľností) je súčasťou výstupu analýzy bezpečnosti, napr. vo forme osobitného dokumentu, ktorý má byť prílohou analýzy bezpečnosti ISVS.

4.2.4. Identifikácia následkov

Následkom sa rozumie hodnota závažnosti ujmy, resp. rozsah škody, ktorá môže byť spôsobená zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou. Pre účely určenia hodnoty negatívnych následkov je možné najprv pomenovať možné následky v kontexte organizácie obdobným spôsobom, ako pri hrozbách či zraniteľnostiach – vo forme katalógu. Vzor katalógu základných negatívnych následkov súvisiacich s ISVS je vytvorený na základe prílohy H štandardu NIST SP 800-30 a upravený pre potreby tejto metodiky analýzy rizík ISVS (je uvedený v prílohe č. 4).

Identifikované typy následkov na aktíva ISVS z dôvodu straty dôvernosti, integrity a dostupnosti môžu byť uvedené v popise konkrétnych scenárov rizík alebo v osobitnom dokumente, ktorý má byť prílohou analýzy bezpečnosti ISVS.

4.2.5. Identifikácia existujúcich bezpečnostných opatrení

Pri výkone analýzy rizík je prostredie organizácie a prevádzky IS skúmané ako jeden celok, vrátane existujúcich bezpečnostných opatrení. Existujúce bezpečnostné opatrenia sú identifikované prevažne vo fáze stanovenia kontextu rizík a vyhodnocované pri určovaní úrovne výsledného rizika.

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 opisoch identifikovaných opatrení na ozrejmenie situácie aj popis aktuálneho stavu daného opatrenia.

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

Identifikácia a popis existujúcich bezpečnostných opatrení vo vzťahu k ISVS majú byť vykonané v každej analyzovanej oblasti bezpečnosti v zmysle štruktúry analýzy bezpečnosti ISVS podľa 4.2.

4.2.6. Identifikácia scenárov rizík

Pred samotným výkonom analýzy rizík sú identifikované všetky podkladové materiály pre popis scenárov rizík, ako sú katalóg aktív, katalóg hrozieb, katalóg zraniteľností a katalóg následkov. Súčasťou tejto fázy je aj identifikácia existujúcich opatrení pre všetky analyzované oblasti bezpečnosti a súvisiace scenáre rizík.

Scenár rizika je postupnosť alebo kombinácia udalostí vedúca od počiatočnej príčiny k nežiaducemu následku.[6] Scenáre rizík predstavujú špecifické situácie realizácie rizík v kontexte vybraných aktív, pričom môžu byť kombináciou viacerých hrozieb a zraniteľností ústiacimi do rôznych následkov.[7] V rámci analýzy rizík ISVS je na identifikáciu scenárov rizík zvolený prístup orientovaný na hrozby, zraniteľnosti, príp. aktíva a následky. V rámci popisu scenárov rizík majú byť popísané okolnosti realizácie daného scenára rizika, príp. uvedené aj konkrétne zistené nedostatky.

Identifikáciu scenárov rizík je potrebné vykonať v každej z analyzovaných oblastí bezpečnosti, pre identifikované scenáre je následne potrebné vyhodnotiť výsledné riziko v kontexte analyzovaného ISVS.

4.3. Identifikácia výsledného rizika

Výsledné riziko sa v identifikovanom scenári určuje ako kombinácia príslušnej hodnoty pravdepodobnosti naplnenia scenára a hodnoty úrovne následkov, ktoré budú mať vo vzťahu k súvisiacim aktívam ISVS. Vzor opisu scenára rizika a s ním súvisiacich opatrení (existujúcich, navrhovaných) je uvedený v prílohe č. 5.

Pri určovaní týchto hodnôt a pri samotnom určovaní výsledného rizika sa vychádza aj z identifikácie existujúcich opatrení implementovaných v IS (tieto majú byť sumarizované v každej analyzovanej oblasti bezpečnosti). V každom scenári rizika sú uvedené odkazy na existujúce opatrenia, ktoré súvisia s daným scenárom a ovplyvňujú hodnoty pravdepodobnosti a následku.

---

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

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

Do týchto hodnôt je implicitne zahrnuté aj kvalitatívne posúdenie existujúcich bezpečnostných opatrení a zistených nedostatkov súvisiacich s daným scenárom.

4.3.1. Určenie pravdepodobnosti naplnenia scenára rizika

Určenie pravdepodobnosti naplnenia scenára rizika je predpokladom na vyhodnotenie daného rizika. Riziko s veľkým následkom, ktoré sa však vyskytne iba raz za dlhý časový horizont môže mať menší negatívny vplyv na bezpečnosť IS ako riziko s nižším následkom, 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 výskytu v stanovenom časovom horizonte (napr. dva roky). V analýze rizík je táto pravdepodobnosť vyjadrená nasledujúcim rozsahom:

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

Pri určovaní pravdepodobnosti sa prihliada aj na ďalšie relevantné informácie k scenáru, napr. frekvenciu výskytu incidentov v minulosti, ktorých podstatou bolo zneužitie príslušnej zraniteľnosti, dostupné štatistické dáta, informácie od jednotiek CSIRT.

4.3.2. Ohodnotenie následkov

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

Následok	Následok popisne
Katastrofický	zásadné ohrozenie výkonu a funkčnosti primárnych procesov, kľúčových aktív; v extrémnom prípade ohrozenie bezpečnosti až existencie kritických aktív vo veľkom rozsahu, resp. celej organizácie
Závažný	prerušenie výkonu určitej konkrétnej služby alebo spôsobenie preukázateľného narušenia bezpečnosti, výdavky na riešenie bezpečnostného incidentu, zvýšené nároky na použitie mimoriadnych personálnych a finančných zdrojov na odstránenie následkov, resp. prerušenie stredne významných činností,

Stredný	následok 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)
Malý	následok neakceptovateľného charakteru, ktorý však môže byť zvládnutý v rámci plnenia bežných pracovných povinností s minimálnymi personálnymi a finančnými nárokmi
Zanedbateľný	následok akceptovateľného charakteru, ktorý môže byť zvládnutý v rámci plnenia bežných pracovných povinností bez potreby dodatočných zdrojov na odstránenie následkov

4.3.3. Určenie úrovne výsledného rizika

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

Pravdepodobnosť	Následok				
	Zanedbateľný	Malý	Stredný	Závažný	Katastrofický
Veľmi vysoká	S	S	V	VV	VV
Vysoká	N	S	V	V	VV
Stredná	N	S	S	V	V
Nízka	VN	N	S	S	S
Veľmi nízka	VN	VN	N	N	S

Klasifikácia závažnosti rizík je vyjadrená stupňom podľa nasledovných významov:

- **VV – veľmi vysoké** – riziko nie je akceptovateľné, riziko bezprostredne a závažne ohrozuje primárne aktíva ISVS, bezpečnosť organizácie, resp. kritického procesu, alebo systému (typicky prekročenie stanoveného limitu tolerancie rizika, katastrofálna finančná strata alebo škoda na majetku, následky na zdravie a život, následky na životné prostredie atď.), prevádzka systému má byť podmienená prijatím ďalších bezpečnostných opatrení na zmiernenie rizika,
- **V – vysoké** – riziko nie je akceptovateľné, riziko závažne ohrozuje primárne aktíva ISVS, bezpečnosť organizácie resp. kritického procesu, alebo systému, ďalšie bezpečnostné opatrenia na jeho zmiernenie by mali byť prijaté, avšak prevádzka systému nie je ním akútne ohrozená vo veľkom rozsahu,
- **S – stredné** – riziko nie je akceptovateľné, riziko potenciálne ohrozuje primárne aktíva ISVS, bezpečnosť organizácie resp. kritického procesu, alebo systému, bezpečnostné opatrenia sú potrebné a mali by byť prijaté v dobe, ktorú určí vlastník rizika,
- **N – nízke** – riziko je akceptovateľné, ale musí byť ďalej priebežne monitorované, riziko neohrozuje primárne aktíva ISVS, ohrozuje výkon niektorých podporných procesov, kritické procesy alebo systémy však nie sú rizikom ohrozené, v niektorých prípadoch môže byť pre toto riziko navrhnuté bezpečnostné opatrenie,

- **VN – veľmi nízke** – riziko je akceptovateľné, nie sú vyžadované žiadne ďalšie bezpečnostné opatrenia, riziko neohrozuje primárne aktíva ISVS, výkon procesov a prevádzka systému nie je rizikom ohrozená.

4.4. Návrh bezpečnostných opatrení

Zostatkové riziko jednotlivých scenárov rizík môže byť v rámci analýzy rizík IS označené ako akceptovateľné, a to najmä z nasledovných príčin:

- pravdepodobnosť jeho realizácie je príliš nízka,
- straty spôsobené jeho realizáciou sú nepatrné,
- realizácia rizika výrazne nenaruší úroveň bezpečnosti stanovenú pre informačný systém,
- opatrenia minimalizujúce pravdepodobnosť jeho realizácie sú nákladnejšie ako prípadné straty,
- opatrenia minimalizujúce pravdepodobnosť jeho realizácie výrazne prevyšujú štandardnú úroveň bezpečnosti v prostredí nasadenia,
- riziko sa netýka informačného systému,
- pri presune rizika na iný subjekt ako prevádzkovateľa IS.

Pre výsledné riziká, ktoré nie sú dostatočne pokryté implementovanými opatreniami (najmä riziká s hodnotami VV a V), sú v tejto analýze bezpečnosti navrhnuté bezpečnostné opatrenia, ktoré dané riziká znižujú na akceptovateľnú úroveň. Pre výsledné riziká s hodnotou S a N je odporúčané ich priebežné sledovanie, v niektorých prípadoch sú pre tieto riziká navrhnuté aj bezpečnostné opatrenia. Riziká hodnoty VN sú akceptovateľné a nevyžadujú si žiadne dodatočné bezpečnostné opatrenia.

V samostatnej prílohe analýzy bezpečnosti ISVS je uvedený prehľadný zoznam všetkých navrhovaných bezpečnostných opatrení podľa jednotlivých analyzovaných oblastí bezpečnosti. Navrhnuté bezpečnostné opatrenia sú klasifikované na kritické (pre riziká s hodnotou VV a V) a nekritické (pre riziká s nižšou hodnotou). Úlohou prevádzkovateľa IS je tieto bezpečnostné opatrenia začleniť do interných procesov riadenia rizík a súvisiacich bezpečnostných opatrení a zabezpečiť ich implementáciu a sledovanie.

Návrh bezpečnostných opatrení vychádza z nasledovných princípov:

- pri návrhu opatrení sa vychádza z výsledného rizika určeného podľa tejto metodiky,
- pre každé výsledné riziko, ktoré nie je akceptovateľné, je popísaný spôsob jeho zníženia pomocou navrhovaných bezpečnostných opatrení,
- cieľom je navrhnúť systém bezpečnostných opatrení takým spôsobom, aby po ich implementácii boli všetky riziká znížené na úroveň zodpovedajúcu akceptovateľným rizikám,

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

- ***Zníženie/redukcia rizika*** – najčastejšia metóda 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).

- ***Vyhnutie sa/obídenie rizika*** – keď je identifikované riziko považované za príliš vysoké, alebo náklady na implementáciu ošetrenia rizika presahujú prínosy, rozhodnutím môže byť 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).
- ***Presun/prenesenie rizika*** – 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),
- ***Akceptácia/zachovanie rizika*** – ak úroveň rizika spĺňa kritériá na akceptáciu rizika, nie je potrebné implementovať opatrenia a riziko môže zostať zachované v pôvodne ohodnotenej úrovni.

Príloha č. 1 – Katalóg aktív

Aktíva sú v katalógu aktív členené v hierarchickej štruktúre vyjadrenej zloženým tvarom identifikátora aktíva. Vyššie v štruktúre sú všeobecnejšie typy aktív, nižšie v štruktúre sú konkrétnejšie typy aktív. Podskupiny aktív predstavujú rôzny náhľad na aktíva, preto je prípustný výskyt aktíva na viacerých miestach katalógu aktív. Konkretizované podskupiny aktív sú zvyčajne uvádzané, ak sa ich týkajú špecifické riziká, inak sa používajú aktíva vyššej úrovne.

Aktíva je tiež možné rozdeliť na:

- primárne – zoskupené pod skupinami A.1 a A.2
- podporné – zoskupené pod skupinami A.3 až A.7

ID	Typ aktíva
A.1	**Poskytované služby**
A.1.1	Služby podľa typu používateľa
A.1.1.1	
A.1.1.2	
A.1.2	Služby podľa úrovne autentifikácie
A.1.2.1	
A.1.2.2	
A.2	**Údaje**
A.2.1	Databázy
A.2.1.1	
A.2.1.2	
A.2.2	Dokumenty ukladané na súborový systém
A.2.3	Autentifikačné údaje
A.2.4	Záznamy z monitorovania
A.2.4.1	
A.2.4.2	
A.2.5	Uložené zálohy údajov
A.2.6	Údaje využívané kryptografickými prostriedkami (kľúče na šifrovanie a elektronický podpis, autentifikačné certifikáty)
A.3	**Zdroje potrebné pre prevádzku**
A.3.1	Personál
A.3.1.1	
A.3.1.2	
A.3.2	Dokumentácia
A.3.2.1	
A.3.2.2	
A.3.3	Priestory a miestnosti
A.3.3.1	Priestory primárneho prevádzkového prostredia

ID	Typ aktíva
A.3.3.2	Priestory záložného prevádzkového prostredia
A.3.4	Spotrebný materiál potrebný na prevádzku
A.3.5	Služby podporných systémov
A.3.5.1	
A.3.5.2	
A.4	**Zariadenia (hardvér) a aplikačné vybavenie (softvér)**
A.4.1	Fyzické servery
A.4.1.1	
A.4.1.2	
A.4.2	Virtualizované servery
A.4.2.1	Webové servery
A.4.2.2	Aplikačné servery
A.4.2.3	
A.4.2.4	
A.4.3	Špecializované zariadenia
A.4.3.1	Load balancery
A.4.3.2	Firewally
A.4.3.3	Diskové polia
A.4.3.4	Páskové knižnice na zálohovanie
A.4.3.5	Záložné zdroje UPS
A.4.3.6	
A.4.4	Virtualizačná platforma
A.4.5	Operačné systémy serverov
A.4.6	Aplikačné vybavenie serverov
A.4.6.1	
A.4.6.2	
A.4.7	Pracovné stanice
A.5	**Aplikačná architektúra**
A.5.1	Modul X
A.5.1.1	Submodul
A.5.1.2	Submodul
A.5.2	Modul Y
A.5.2.1	Submodul
A.5.2.2	Submodul
A.5.3	Podporné moduly
A.5.3.1	
A.5.3.2	
A.5.4	Prevádzkové prostredia
A.5.4.1	Primárne produkčné prostredie
A.5.4.2	Záložné prostredie

ID	Typ aktíva
A.5.4.3	Testovacie a školiace prostredie
A.5.4.4	Vývojové prostredie
A.6	**Sieťové prostredie**
A.6.1	Logické segmenty siete v primárnom dátovom centre
A.6.1.1	Demilitarizovaná zóna (DMZ)
A.6.1.2	Aplikačný segment
A.6.1.3	Dátový segment
A.6.1.4	Manažment segment
A.6.1.5	Klientsky segment
A.6.1.6	
A.6.2	Logické segmenty siete vytvorené v záložnom dátovom centre
A.6.3	Ostatné časti vnútornej siete
A.6.4	Podporná sieťová infraštruktúra (aktívne sieťové prvky, kabeláž)
A.6.5	
A.6.6	
A.7	**Integrácie na iné informačné systémy**
A.7.1	
A.7.2	

Príloha č. 2 – Katalóg hrozieb

Katalóg hrozieb je zoznam všetkých dôvodne očakávaných hrozieb súvisiacich s organizáciou, resp. vyvíjaným IS, ktorý napomáha pri identifikácii hrozieb využitím existujúcej taxonómie v kontexte konkrétnych scenárov rizík.

Národný bezpečnostný úrad spracoval návrh verejného katalógu hrozieb, ktorý je možné použiť aj pre účely bezpečnostného projektu ISVS. Ako zdrojové verejné katalógy hrozieb slúžili tiež:

- ENISA Threat Taxonomy – katalóg hrozieb z výročnej správy Agentúry Európskej únie pre kybernetickú bezpečnosť Threat Landscape (ETL) o stave hrozieb kybernetickej bezpečnosti,
- štandard STN ISO/IEC 27005:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti,
- National Institute of Standards & Technology (NIST) SP 800-30,
- Bundesamt fur Sicherheit in der Informationstechnik (BSI) IT- Grundschutz-Katalog.

Pôvod hrozieb je uvádzaný v zmysle požiadavky § 6 ods. 10 vyhlášky NBÚ č. 362/2018 Z. z. (D – úmyselná, A – náhodná, E – vplyv prostredia).[8]

Kód hrozby	Hrozba	Popis hrozby (typický príklad)	Pôvod
H.1	**Fyzické hrozby**		
H.1.1	Oheň	Poškodenie (typicky nosičov údajov, alebo IT zariadení) požiarom	A, D, E
H.1.2	Prach, korózia, mrazy	Poškodenie (typicky nosičov údajov, alebo IT zariadení) prachom, mrazom, koróziou	A, D, E
H.1.3	Veľká nehoda	Poškodenie (typicky nosičov údajov, alebo IT zariadení) alebo obmedzenie funkcií z dôvodu vplyvu okolitých blízkych udalostí (napríklad únik radiácie, požiar vedľajšej budovy, chemické znečistenie, výbuch v blízkosti, dopravná nehoda, letecká nehoda) vrátane ďalších následkov vyplývajúcich z udalosti - cestné uzávery, zákaz vychádzania a podobne	A, D, E
H.1.4	Voda	Poškodenie (typicky nosičov údajov, alebo IT zariadení) záplavou, vytopením, typicky vodoinštalačnou haváriou	A, D, E
H.1.5	Výbuch	Priemyselná havária, bombový útok, teroristické útoky, vojna, použitie zbraní	A, D, E
H.1.6	Znečistenie, škodlivé žiarenie	Poškodenie (typicky nosičov údajov, alebo IT zariadení) znečistením alebo škodlivým elektromagnetickým žiarením	A, D, E
H.1.7	Zničenie zariadenia, alebo médií	Zničenie zariadení, alebo médií napr. vodou, požiarom, vandalizmus, zlyhanie úložného zariadenia, atď.	A, D, E

[8] z angl. prekladu Deliberate, Accidental, Environmental

H.2	**Hospodárske a ekonomické hrozby**		
H.2.1	Chybný rozpočet	Nedostatky finančného rozpočtu	A, D
H.2.2	Energetická závislosť	Nediverzifikovaná závislosť na jednom dodávateľovi energie, resp. zdrojov na jej výrobu	A, E
H.2.3	Narušenie hospodárstva štátu	Narušenie alebo obmedzenie menového, devízového a finančného hospodárstva	D
H.2.4	Ekonomické ovplyvňovanie tretej strany	Politické riziko tretej strany vzhľadom na analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany	D
H.3	**Informačné operácie**		
H.3.1	Šírenie propagandy	Úmyselné šírenie propagandy za účelom ovplyvňovania mienky v neprospech záujmu organizácie	D
H.3.2	Vytvorenie dezinformácií	Úmyselné vytvorenie a ďalšie šírenie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu organizácie	D
H.3.3	Zdieľanie dezinformácií	Zdieľanie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu organizácie	D
H.4	**Kompromitácia funkcií alebo služieb**		
H.4.1	Chyba pri používaní	Nechcená modifikácia údajov v databázach, zmazanie súborov, potrebných pre chod softvéru, chyba operátora, ktorý modifikuje údaje, vysoké pracovné zaťaženie, stres alebo negatívne zmeny pracovných podmienok, zadanie úlohy nad rámec schopností zamestnanca, slabé znalosti a zručnosti, atď.	A
H.4.2	Chyby prenosu (vrátane nesprávneho smerovania správ)	Reorganizácia prenosových kanálov elektronických, alebo materializovaných údajov; zmena pracovného jazyka, zmeny v doručovaní pošty, úprava alebo presmerovanie správ, atď.	D
H.4.3	Falšovanie práv alebo povolení	Neoprávnené pozmeňovanie identít a prístupových práv do systémov, a ich zneužitie na podvodné konanie v mene iného používateľa	D
H.4.4	Odmietnutie konania	Odmietnutie vykonania pracovnej aktivity, odopretie pracovnej zodpovednosti v procese, štrajk, atď.	D
H.4.5	Odmietnutie služby	Narušenie procesov, infraštruktúry alebo iných prvkov za účelom znefunkčnenia služby (typicky DoS, DDoS)	A, D
H.4.6	Zhoršovanie stavu pamäťových médií	Starnutie archivovaných dokumentov, postupné prepisovanie obsahu v čase, dobrovoľné vymazanie častí dokumentu, zničenie médií napr. pri požiari, záplave atď.	A, E
H.4.7	Zneužitie práv alebo povolení	Neoprávnené získanie identít a prístupových práv do systémov, a ich zneužitie na podvodné konanie v mene iného používateľa	A, D
H.5	**Ľudské konanie**		

H.5.1	Popretie	Popretie pôvodu informácie (neoprávnené popretie pravdivej informácie). Tiež stav, keď aplikácia alebo systém neprijme informáciu o zaznamenávaní aktivity používateľa, čo umožňuje zlomyseľnú manipuláciu alebo sfalšovanie identifikácie aktivít. Hrozba útoku na platnosť a integritu akcií v aplikácii. Manipulácia alebo sfalšovanie identifikácie nepovolených aktivít, vymazanie denníkov alebo zápis nesprávnych údajov do protokolových súborov	A, D
H.5.2	Detekcia polohy	Zistenie údajov o geografickej polohe	D
H.5.3	Infiltrácia webovej komunikácie	Poškodenie, alebo neoprávnená zmena obsahu, typicky webovej stránky, alebo aplikácie, ktoré môže zmeniť informačný obsah, alebo aj vizuálny vzhľad webovej stránky, alebo aplikácie (tzv. defacement). Hrozba prieniku do cieľového systému prostredníctvom webových aplikácií.	D
H.5.4	Krádež digitálnej identity alebo prihlasovacích údajov	Krádež identity a jej zneužitie na podvodné konanie alebo neoprávnený prístup.	D
H.5.5	Krádež médií alebo dokumentov	Krádež dokumentov, krádež súborov, strata súborov počas sťahovania, krádež emailu z mailboxu, rozmnožovanie dokumentov počas prenosu, nájdenie stratených dokumentov, atď.	D
H.5.6	Krádež zariadenia	Krádež notebooku, alebo mobilu, strata zariadenia, nájdenie strateného zariadenia, strata úložného zariadenia, atď.	D
H.5.7	Manipulácia s hardvérom	Neoprávnená manipulácia s hardvérom, pridanie nekompatibilnej časti zariadenia, ktoré vedie k nefunkčnosti, odobratie komponentov, potrebných pre správne fungovanie systému, sledovanie hardvérovým keyloggerom, odstránenie komponentov zariadenia, pripojenie zariadení (napr.: USB diskov) pre štart OS alebo získanie dát, použitie USB kľúčov alebo diskov, ktoré nie sú vhodné pre danú klasifikáciu informácií, použitie alebo prenos citlivých zariadení pre osobné použitie, ukladanie súkromných súborov, osobné použitie atď.	D
H.5.8	Manipulácia so softvérom	Neoprávnená manipulácia so softvérom, nepovolené, neschválené aktualizácie, konfigurácie, výmena komponentov, nelegálne spájanie údajov, nepovolené získanie vyšších oprávnení, mazanie stôp po použití, zneužite softvérových funkcií, atď.	A, D
H.5.9	Neoprávnené používanie zariadení	Neoprávnený alebo neautorizovaný prístup do systému alebo k zariadeniu, znižovanie zabezpečenia zariadení a služieb	D
H.5.10	Neoprávnené spracúvanie osobných údajov	Neoprávnené poskytnutie, sprístupnenie alebo zverejnenie osobných údajov o inom zhromaždené v súvislosti s výkonom verejnej moci alebo uplatňovaním ústavných práv osoby, alebo získaných v súvislosti s výkonom svojho povolania, zamestnania alebo funkcie	A, D
H.5.11	Neoprávnený vstup do priestorov	Neoprávnený fyzický vstup do priestorov	D
H.5.12	Nesprávne používanie zariadení	Porušenie politík alebo návodov na bezpečné používanie zariadenia	A, D

H.5.13	Nezákonné spracovanie údajov	Neoprávnená manipulácia s informáciami	D
H.5.14	Odosielanie alebo distribúcia malvéru	Infiltrácia škodlivým kódom, výmaz spúšťacích súborov alebo zdrojového kódu, atď.	A, D, E
H.5.15	Odpočúvanie	Sledovanie cudzej obrazovky, odfotenie cudzej obrazovky, GPS sledovanie zariadenia, vzdialená detekcia elektromagnetického signálu, (vrátane analýzy dátovej prevádzky) atď.	D
H.5.16	Podvodné kopírovanie softvéru	Neoprávnená manipulácia so softvérom vedúca k nepovolenému/neschválenému kopírovaniu kódu, prípadne až ku odcudzeniu kódu.	D
H.5.17	Poškodenie reputácie	Poškodenie reputácie úmyselným konaním (klebety, ohováranie, dezinformácie, dehonestácia predstaviteľov organizácie, poškodzovanie dobrého mena atď.)	A, D
H.5.18	Poškodenie údajov	Zmena, alebo zničenie údajov, zmena hodnôt v súbore, nahradenie originálnych hodnôt falšovanými, zmeny údajov bez vedomia autora, odosielanie viacerých konfliktných dokumentov, manipulácia alebo zmena s informáciou, ktorá znamená narušenie jej integrity.	D
H.5.19	Poškodenie zariadení alebo médií	Úmyselné poškodenie zariadení, alebo médií, narušenie integrity zariadenia alebo média.	A, D
H.5.20	Používanie falošného alebo skopírovaného softvéru	Použitie nelegálneho, falošného alebo nelicencovaného softvéru. Tento je typicky upravený tak, aby obsahoval malvér ohrozoval počítačový systém	A, D
H.5.21	Používanie sieťových zariadení neoprávneným spôsobom	Skenovanie sieťových adries a portov, zbieranie konfiguračných dát, analýza zdrojového kódu za účelom lokalizovať slabé miesta, testovanie databáz na reakciu na poškodzujúce dotazy, atď.	D
H.5.22	Prístup neoprávneného používateľa k sieti	Skenovanie sieťových adries a portov, hľadanie zraniteľností pri počúvaní, analýze, reportovaní alebo sprostredkovacie porty a služby	D
H.5.23	Sociálne inžinierstvo	Zneužitie práv, ovplyvňovanie (phishing, sociálne inžinierstvo, podplácanie, a pod.), nátlak (výhražné emaily, psychologické obťažovanie) atď.	D
H.5.24	Teroristický útok, sabotáž	Úmyselná manipulácia alebo poškodenie fyzických objektov, zariadení a/alebo procesov alebo obmedzenie funkcií z dôvodu sabotáže, alebo teroristického útoku, za účelom spôsobenia škody	D
H.5.25	Útok man-in-the-middle	Typ hrozby počas ktorej útočník prenikne do komunikácie medzi dvoma účastníkmi a bez ich vedomia začne komunikáciu neoprávnene modifikovať	D
H.5.26	Vstup údajov z nedôveryhodných zdrojov	Údaje získané z nedôveryhodných zdrojov, kompromitácia údajov, atď. (Napr. prezenčná listina bez súhlasov, používanie mailinglistu s neoprávnene získanými, alebo chybnými adresami)	A, D
H.5.27	Vzdialené špehovanie	Špehovanie sieťovej prevádzky, získavanie dát posielaných cez rádiofrekvenčné siete, maskovanie identity, sledovanie softvérovým keyloggerom, infekcia škodlivým kódom, inštalácia nástroja na vzdialenú správu, výmena pôvodných komponentov, atď.	D

H.5.28	Zachytenie žiarenia zariadenia	Sledovanie GPS signálu zariadenia, vzdialená detekcia elektromagnetického vyžarovania zariadenia, vrátane analýzy dátovej prevádzky atď.	D
H.5.29	Zber recyklovaných alebo vyradených médií	Nedostatočné zmluvy o vyradení a údržbe zariadení, resp. nedostatočné, alebo chybné procedúry vyradenia a údržby môžu viesť k neoprávnenému prístupu k informáciám	D
H.5.30	Neoprávnené zverejňovanie informácií	Neoprávnené zverejnenie informácií v rozpore bezpečnostnými opatreniami prijatými na základe klasifikácie informácií, osobám, ktoré k nim nemajú mať prístup, resp. v rozpore s legislatívnymi požiadavkami (napr. zverejňovanie zdrojového kódu podľa zákona o ITVS, obsahujúce však citlivé informácie ako sú heslá či osobné údaje)	A, D
H.6	**Medzinárodné vzťahy**		
H.6.1	Neplnenie záväzkov EÚ	Neplnenie alebo obmedzené plnenie záväzkov zo zmlúv s EÚ, ktorými je Slovenská republika viazaná, alebo obmedzovanie členstva v medzinárodných organizáciách	D
H.6.2	Neplnenie záväzkov NATO	Neplnenie alebo obmedzené plnenie záväzkov zo zmlúv s NATO, ktorými je Slovenská republika viazaná, alebo obmedzovanie členstva v medzinárodných organizáciách	D
H.6.3	Neplnenie záväzkov OSN	Neplnenie alebo obmedzené plnenie záväzkov zo zmlúv s OSN, ktorými je Slovenská republika viazaná, alebo obmedzovanie členstva v medzinárodných organizáciách	D
H.7	**Obrana štátu**		
H.7.1	Asymetrické útoky	Asymetrická (rozvratná, sabotážna a spravodajská) aktivita voči Slovenskej republike	D
H.7.2	Obmedzenie mobilizácie	Obmedzenie, alebo znemožnenie procesu mobilizácie	D
H.7.3	Obmedzenie prípravy obrany štátu	Znemožnenie alebo obmedzenie prípravy obrany štátu v podobe ľudského, materiálneho a organizačného charakteru	D
H.7.4	Obmedzenie vojenských operácií	Obmedzenie alebo znemožnenie vykonávania vojenských operácií	D
H.8	**Organizačné hrozby**		
H.8.1	Chybné plánovanie a nedostatky v adaptácii	Zanedbanie bezpečnostných požiadaviek pri plánovaní, nákupe a implementácii zariadení, služieb a procesov	A, D
H.8.2	Nedostatok personálu	Preloženie, ukončenie kontraktu alebo zrušenie, prevzatie firmy alebo jej časti, prevzatie zamestnanca, zmena zaradenia, ukončenie procesu po organizačnej zmene, doručenie pošty zrušené štrajkom, pracovný úraz, choroba z povolania, iné zranenie alebo choroba, smrť, neurologická, psychologická alebo psychiatrická diagnóza, atď. atď.	A, E
H.8.3	Nedostatok zdrojov	Nedostatok alebo nesprávne riadenie finančných, technických alebo personálnych zdrojov	A, E

H.8.4	Porušenie interných riadiacich aktov	Nesúlad s platnými porušenia internými riadiacimi aktami vyúsťujúce do potenciálneho incidentu	A, D
H.8.5	Porušenie zákonov alebo nariadení	Nesúlad s platnou reguláciou, porušenie zákona vyúsťujúce do trestno-právnej, správno-právnej alebo inej právnej konzekvencie	A, D
H.8.6	Zlyhanie poskytovateľov služieb	Prerušenie outsourcovaných služieb, napr. dodávky plynu, elektrickej energie, telekomunikačných služieb, vody, ventilácie atď.	A, E
H.9	**Poruchy infraštruktúry**		
H.9.1	Elektromagnetická radiácia	Poškodenie údajov (typicky na nosičoch) elektromagnetickým žiarením, radiáciou	A, D, E
H.9.2	Elektromagnetické impulzy	Poškodenie údajov (typicky na nosičoch) elektromagnetickými impulzmi, resp. kolísaním napájania	A, D, E
H.9.3	Porucha chladiaceho alebo ventilačného systému	Porucha klimatizácie alebo prívodu vody ktoré môže spôsobiť výpadky systémov a následne zníženie úrovne dostupnosti údajov	A, D
H.9.4	Porucha napájacieho systému	Narušenie alebo poškodenie energetickej infraštruktúry	A, D
H.9.5	Porucha telekomunikačného zariadenia	Zlyhanie telekomunikačných komponentov, prerušenie kabeláže, slabý telekomunikačný signál, nedostatočný signál Wi-Fi, atď.	A, D
H.9.6	Porucha telekomunikačnej siete	Poškodenie telekomunikačného spojenia, zničenie kabeláže, výpadok komponentov optického spojenia, nedostupné WiFi pripojenie, atď.	A, D, E
H.9.7	Strata napájania	Obmedzená alebo zastavená dodávka energií resp. zdrojov na jej výrobu	A, D, E
H.9.8	Tepelné žiarenie	Poškodenie údajov (typicky na nosičoch) tepelným žiarením, infračerveným žiarením, neprimeranou teplotou	A, D, E
H.10	**Prírodné hrozby**		
H.10.1	Klimatický jav	Poškodenie (typicky nosičov údajov, alebo IT zariadení) alebo obmedzenie funkcií z dôvodu klimatického javu - tornádo, záplava, zosuv pôdy, lavína, lesný požiar	E
H.10.2	Meteorologický jav	Poškodenie (typicky nosičov údajov, alebo IT zariadení) mrazom, vysokou teplotou, vetrom, vlhkosťou, bleskom	E
H.10.3	Pandémia/epidemický jav	Rozsiahla epidémia, nemoc, ktorá sa rozširuje na geograficky rozsiahlom území a spôsobuje typicky nedostupnosť personálu	E
H.10.4	Poškodenie zvieraťom	Poškodenie (typicky nosičov údajov, alebo IT zariadení) zvieratami	A, E
H.10.5	Povodeň	Poškodenie (typicky nosičov údajov, alebo IT zariadení) povodňou	E
H.10.6	Seizmický jav	Poškodenie (typicky priestorov, nosičov údajov, alebo IT zariadení) zemetrasením, alebo inými seizmickými udalosťami	E
H.10.7	Sopečný fenomén	Poškodenie (typicky priestorov, nosičov údajov, alebo IT zariadení)vulkanickými udalosťami	E
H.11	**Štátna nezávislosť a rozhodovanie**		

H.11.1	Obmedzenie rozvoja	Obmedzenie alebo znemožnenie politického, ekonomického, sociálneho a vojenského rozvoja Slovenskej republiky	D
H.11.2	Špionáž	Zhromažďovanie, vyhodnocovanie a spracovanie informácií neoprávneným spôsobom, v neprospech štátneho zriadenia	D
H.11.3	Negatívne spravodajské informácie	Hrozby vyplývajúce z informácií špecifických pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky	D
H.11.4	Strata slobody rozhodovania	Strata slobody rozhodovania a konania na strategickom, operačnom a taktickom stupni štátu zo strany predstaviteľov verejne moci	D
H.11.5	Znemožnenie presadzovania záujmov	Znemožnenie presadzovania záujmov (národno-štátnych, organizačných) na medzinárodnej úrovni	D
H.11.6	Ovplyvňovanie a zasahovanie do činnosti tretej strany cudzím štátom	Možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy (ďalej len „cudzí štát“)	D
H.11.7	Negatívne informácie z analýzy právnych predpisov cudzieho štátu	Politické riziko tretej strany vzhľadom na analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií	D
H.12	**Súkromie**		
H.12.1	Detekovateľnosť	Potenciál, že útočník dokáže z uložených údajov dostatočne rozlíšiť, či predmet záujmu, resp. položka množiny jestvuje alebo nie. (napr. schopnosť rozpoznania súborov obsahujúcich osobné údaje od iných typov údajov)	A, D
H.12.2	Identifikovateľnosť	Potenciál, že útočník dokáže priamo identifikovať dotknuté osoby asociované na predmety záujmu (napr. v súbore osobných údajov rozpoznať osobné údaje konkrétnej dotknutej osoby. napr. konkrétneho odosielateľa správy medzi mnohými správami elektronickej pošty). Identifikovateľnosť je špeciálny typ spojiteľnosti, kde sú zahrnuté aj atribúty dotknutých osôb.	A, D
H.12.3	Nepopierateľnosť	Potenciál, že útočník dokáže z podstaty procesu zhromaždiť dôkazy proti nárokom odporujúcej strany a dokázať, že používateľ vie, že niečo urobil, alebo že niečo povedal. Opakom je plausible deniability (tzv. prijateľné popretie - t.j. neoprávnené zverejňovanie pravdivej informácie, resp. pôvodu informácie, napr. dotknutá osoba nechce, aby bolo jasné, komu dala hlas vo voľbách do DR, avšak útočník túto informáciu zverejní)	A, D
H.12.4	Nesúlad s právnym základom	Nesúlad spracovania s politikami a právnym základom (napr. poskytnutým súhlasom) je hrozba, ktorá znamená, že napriek deklarácii súladu spracovania s politikami, neexistuje záruka, že systém skutočne vyhovuje prijatým pravidlám. Tým následne môže nastať porušenie práv dotknutej osoby.	A, D

H.12.5	Neznalosť klasifikácie	Neznalosť klasifikácie je hrozba, ktorá indikuje, že používateľ si neuvedomuje citlivosť, resp. klasifikačný stupeň informácie spracovanej v systéme a následne napr. zverejňuje informácie, ktoré umožnia potenciálnemu útočníkovi zistiť napr. identitu používateľa. Alebo naopak - používateľ poskytuje nepresné informácie, ktoré môžu následne spôsobiť nesprávne rozhodnutia alebo akcie. (napr. nechcené prezradenie informácií)	A, D
H.12.6	Neznalosť obsahu	Neznalosť obsahu je hrozba, ktorá indikuje, že používateľ si neuvedomuje obsah informácie spracovanej v systéme a následne napr. zverejňuje nadbytočné informácie, ktoré umožnia potenciálnemu útočníkovi zistiť napr. identitu používateľa. Alebo naopak - používateľ poskytuje nepresné informácie, ktoré môžu následne spôsobiť nesprávne rozhodnutia alebo akcie. (napr. nechcené prezradenie informácií)	A, D
H.12.7	Neoprávnené sprístupnenie	Neoprávnené sprístupnenie osobných údajov v rozpore bezpečnostnými opatreniami prijatými na základe klasifikácie informácií, osobám, ktoré k nim nemajú mať prístup. (Neoprávnené prečítanie, kopírovanie, fotografovanie, použite odpočúvacích zariadení na stretnutiach, atď.)	A, D
H.12.8	Spojiteľnosť, linkovateľnosť	Spojiteľnosť (linkovateľnosť) je hrozba, že útočník dokáže aj nepriamo rozpoznať podstatu entity, alebo vzájomné vzťahy entít. (napr. odosielateľa podľa domény, aktivity, alebo podľa predmetu správy)	A, D
H.13	**Technické poruchy**		
H.13.1	Porucha softvéru	Chyby počas aktualizácie, konfigurácie alebo údržby, infekcia škodlivým kódom, výmena komponentov, neobnovenie licencie na softvér používaný na prístup k údajom, atď.	A, D
H.13.2	Porucha zariadenia alebo systému	Náhle a neplánované zlyhanie alebo porucha IT zariadenia, alebo akéhokoľvek HW komponentu, ktoré môže spôsobiť zníženie úrovne dostupnosti údajov	A
H.13.3	Strata napájania alebo kolísanie výkonu	Strata zdroja napájania alebo kolísanie výkonu napájania zariadení	A, D, E
H.13.4	Zahltenie informačného systému	Plná úložná jednotka, výpadok el. energie, preťaženie systému, prehriatie, výnimočné teploty, atď.	A, D
H.13.5	Zníženie úrovne údržby, chyba údržby informačného systému	Neplánované zníženie úrovne údržby systémov, chyba údržby informačného systému, alebo IT zariadení	A, D
H.14	**Územná celistvosť a nedotknuteľnosť hraníc**		
H.14.1	Strata kontroly nad územím	Strata kontroly na časťou, alebo celým územím Slovenskej republiky	D
H.14.2	Strata obyvateľstva	Strata obyvateľstva v dôsledku vojenských aktivít alebo iných aktivít porušujúcich medzinárodné právo	D

H.14.3	Strata zdrojov	Strata kritických prírodných, potravinových, hospodárskych, infraštruktúrnych, energetických a dopravných zdrojov a spôsobilostí Slovenskej republiky	D
H.15	**Verejný poriadok**		
H.15.1	Destabilizácia	Destabilizácia a narušenie chodu orgánov verejnej moci	D
H.15.2	Poškodenie zdravia obyvateľstva	Poškodenie zdravia a/alebo úmrtie významnej časti obyvateľov v dôsledku narušenia verejného poriadku	D
H.15.3	Preťaženie dopravy	Preťaženie kapacity prevádzky - preťaženie pošty, preťaženie procesov overovania, prekročenie veľkosti databázy, vkladanie dát mimo normálny rozsah hodnôt, zneužite šírky pásma, neoprávnené sťahovanie, strata internetovej konektivity, atď.	D
H.15.4	Verejné nepokoje	Verejné nepokoje a protesty, vedúce k narušeniu verejného poriadku na území okresu, kraja, štátu	D
H.15.5	Významné spoločenské udalosti v okolí	Poškodenie (typicky nosičov údajov, alebo IT zariadení) alebo obmedzenie funkcií z dôvodu významných udalostí v okolí, vyvolaných ľudskou činnosťou (športové udalosti, festivaly atď.)	D

Príloha č. 3 – Katalóg zraniteľností

Podkladový katalóg zraniteľností vychádza zo štandardu STN ISO/IEC 27005:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia – Usmernenie k riadeniu rizík informačnej bezpečnosti.

Oblasť	ID	Zraniteľnosť
1. Hardvér	Z.1.1	Nedostatočná údržba/chybná inštalácia pamäťových médií
	Z.1.2	Nedostatočné plány pravidelnej výmeny zariadení
	Z.1.3	Náchylnosť na vlhkosť, prach a znečistenie
	Z.1.4	Citlivosť na elektromagnetické žiarenie
	Z.1.5	Nedostatočná kontrola zmien konfigurácií
	Z.1.6	Citlivosť na zmeny napätia
	Z.1.7	Citlivosť na zmeny teploty
	Z.1.8	Nechránené ukladanie
	Z.1.9	Nedostatok starostlivosti pri likvidácii
	Z.1.10	Nekontrolované kopírovanie
2. Softvér	Z.2.1	Žiadne alebo nedostatočné testovanie softvéru
	Z.2.2	Známe chyby v softvéri
	Z.2.3	Žiadne „odhlásenie“ pri opustení pracovnej stanice
	Z.2.4	Likvidácia alebo opätovné použitie pamäťových médií bez riadneho vymazania
	Z.2.5	Nedostatočná konfigurácia logov na účely auditného záznamu
	Z.2.6	Nesprávne pridelenie prístupových práv
	Z.2.7	Široko distribuovaný softvér
	Z.2.8	Použitie aplikačných programov na nesprávne údaje z časového hľadiska
	Z.2.9	Komplikované používateľské rozhranie
	Z.2.10	Nedostatočná alebo chýbajúca dokumentácia
	Z.2.11	Nesprávne nastavenie parametrov
	Z.2.12	Nesprávne dátumy
	Z.2.13	Nedostatočné identifikačné a autentifikačné mechanizmy (napr. na overenie používateľa)
	Z.2.14	Nechránené tabuľky hesiel
	Z.2.15	Slabá správa hesiel
	Z.2.16	Povolené nepotrebné služby
	Z.2.17	Nevyspelý alebo nový softvér
	Z.2.18	Nejasné alebo neúplné špecifikácie pre vývojárov
	Z.2.19	Neúčinná kontrola zmien
	Z.2.20	Nekontrolované sťahovanie a používanie softvéru
	Z.2.21	Nedostatok alebo neúplnosť záložných kópií
	Z.2.22	Nevypracovanie správ o riadení
3.Sieť	Z.3.1	Nedostatočné mechanizmy na preukázanie odoslania alebo prijatia správy

	Z.3.2	Nechránené komunikačné linky
	Z.3.3	Nechránená citlivá prevádzka
	Z.3.4	Zlá spoločná kabeláž
	Z.3.5	Jediný bod zlyhania
	Z.3.6	Neúčinné alebo chýbajúce mechanizmy na identifikáciu a overenie odosielateľa a príjemcu
	Z.3.7	Nezabezpečená sieťová architektúra
	Z.3.8	Prenos hesiel v čitateľnom stave
	Z.3.9	Nedostatočné riadenie siete (odolnosť smerovania)
	Z.3.10	Nechránené verejné sieťové pripojenia
4. Personál	Z.4.1	Neprítomnosť personálu
	Z.4.2	Nedostatočné postupy pri prijímaní zamestnancov
	Z.4.3	Nedostatočné bezpečnostné školenia
	Z.4.4	Nesprávne používanie softvéru a hardvéru
	Z.4.5	Slabé povedomie o bezpečnosti
	Z.4.6	Nedostatočné alebo chýbajúce mechanizmy monitorovania
	Z.4.7	Práca bez dozoru externých alebo upratovacích pracovníkov
	Z.4.8	Neúčinné alebo chýbajúce zásady správneho používania telekomunikačných médií a zasielania správ
5. Lokalita	Z.5.1	Nedostatočné alebo nedbalé používanie fyzických opatrení do budov a miestností
	Z.5.2	Poloha v oblasti náchylnej na povodeň
	Z.5.3	Nestabilná elektrická sieť
	Z.5.4	Nedostatočná fyzická ochrana budov, dverí a okien
6. Organizačné prostredie	Z.6.1	Formálny postup registrácie a zrušenia registrácie používateľov nie je vypracovaný alebo jeho vykonávanie je neúčinné
	Z.6.2	Formálny proces preskúmania prístupových práv (dohľad) nie je vypracovaný alebo jeho vykonávanie je neúčinné
	Z.6.3	Nedostatočné ustanovenia (týkajúce sa bezpečnosti) v zmluvách so zákazníkmi a/alebo tretími stranami
	Z.6.4	Postup monitorovania zariadení na spracovanie informácií nie je vypracovaný alebo jeho vykonávanie je neúčinné
	Z.6.5	Audity (dohľad) sa nevykonávajú pravidelne
	Z.6.6	Postupy identifikácie a posúdenia rizík nie sú vypracované alebo ich vykonávanie je neúčinné
	Z.6.7	Nedostatočné alebo chýbajúce hlásenia o poruchách zaznamenané v logoch správcu a operátora
	Z.6.8	Neprimeraná reakcia na servisnú údržbu
	Z.6.9	Nedostatočná alebo chýbajúca dohoda o úrovni služieb
	Z.6.10	Postup kontroly zmien nie je vypracovaný alebo jeho vykonávanie je neúčinné
	Z.6.11	Formálny postup kontroly dokumentácie ISMS nie je vypracovaný alebo jeho implementácia je neúčinná
	Z.6.12	Formálny postup pre dohľad nad záznamami ISMS nie je vypracovaný alebo jeho vykonávanie je neúčinné
	Z.6.13	Formálny proces autorizácie verejne dostupných informácií nie je vypracovaný alebo jeho vykonávanie je neúčinné
	Z.6.14	Nesprávne rozdelenie zodpovednosti za informačnú bezpečnosť
	Z.6.15	Plány kontinuity neexistujú, sú neúplné alebo zastarané

	Z.6.16	Politika používania elektronickej pošty nie je vypracovaná alebo jej vykonávanie je neúčinné
	Z.6.17	Postupy zavádzania softvéru do prevádzkových systémov nie sú vypracované alebo ich implementácia je neúčinná
	Z.6.18	Postupy pre manipuláciu s klasifikovanými informáciami nie sú vypracované alebo ich vykonávanie je neúčinné
	Z.6.19	Povinnosti v oblasti informačnej bezpečnosti nie sú uvedené v opisoch pracovných miest
	Z.6.20	Nedostatočné alebo chýbajúce ustanovenia (týkajúce sa informačnej bezpečnosti) v zmluvách so zamestnancami
	Z.6.21	Disciplinárny postup v prípade incidentu v oblasti informačnej bezpečnosti nie je definovaný alebo nefunguje správne
	Z.6.22	Formálna politika používania mobilných počítačov nie je vypracovaná alebo jej uplatňovanie je neúčinné
	Z.6.23	Nedostatočná kontrola aktív mimo pracoviska
	Z.6.24	Nedostatočná alebo chýbajúca politika „čistého stola a čistej obrazovky“
	Z.6.25	Autorizácia zariadení na spracovanie informácií nie je zavedená alebo nefunguje správne
	Z.6.26	Mechanizmy monitorovania narušení bezpečnosti nie sú riadne zavedené
	Z.6.27	Postupy na nahlasovanie bezpečnostných nedostatkov nie sú vypracované alebo ich vykonávanie je neúčinné
	Z.6.28	Postupy dodržiavania ustanovení o duševných právach nie sú vypracované alebo ich uplatňovanie je neúčinné

Príloha č. 4 – Katalóg následkov

Vzor katalógu základných negatívnych následkov súvisiacich s ISVS je vytvorený na základe prílohy H štandardu NIST SP 800-30 a upravený pre potreby tejto metodiky analýzy rizík ISVS. Pomenovanie možných následkov na základe tohto katalógu je v rámci definovanej metodiky voliteľné a má využitie najmä pri určovaní výslednej hodnoty negatívnych následkov.

Oblasť	ID	Následok
1. Následky na prevádzku	N.1.1	Neschopnosť alebo čiastočná neschopnosť vykonávať súčasné procesy prevádzky
	N.1.2	Úplná alebo čiastočná neschopnosť vykonávať procesy prevádzky v budúcnosti
	N.1.3	Odmietnutie vykonať službu alebo nedostupnosť služby
	N.1.4	Nedodržanie stanovenej lehoty pre vykonanie služby
	N.1.5	Dodatočné finančné náklady na prevádzku
	N.1.6	Zhoršenie efektívnosti riadenia prevádzky a bezpečnosti
	N.1.7	Zvýšený potenciál pre vznik bezpečnostných incidentov
2. Následky na prvky IS a prevádzkovateľa	N.2.1	Poškodenie alebo strata fyzických priestorov a ich vybavenia
	N.2.2	Poškodenie alebo straty na úrovni informačných systémov a sietí
	N.2.3	Poškodenie alebo straty technologického vybavenia
	N.2.4	Poškodenie alebo strata údajov
	N.2.5	Neoprávnený prístup k údajom
	N.2.6	Porušenie legislatívnych, zmluvných alebo iných záväzných predpisov
	N.2.7	Narušenie dôveryhodnosti a dobrého mena prevádzkovateľa
3. Následky na ľudské zdroje	N.3.1	Zranenia alebo straty na životoch
	N.3.2	Zlé fyzické alebo psychické zaobchádzanie
	N.3.3	Krádež identity
	N.3.4	Strata osobných údajov
	N.3.5	Poškodenie osobnej reputácie
	N.3.6	Zvýšené nároky na personál
4. Následky na tretie strany	N.4.1	Negatívne ovplyvnenie prevádzky informačných systémov tretej strany
	N.4.2	Priame finančné náklady pre tretiu stranu
	N.4.3	Poškodenie dobrých vzťahov s tretími stranami
	N.4.4	Porušenie zmluvy s treťou stranou
	N.4.5	Súdne konania a sankcie
5. Následky na národnej úrovni	N.5.1	Poškodenie kritickej infraštruktúry štátu
	N.5.2	Narušenie kontinuity činností zložiek riadenia štátu
	N.5.3	Strata súčasnej či budúcej schopnosti štátu napĺňať stanovené úlohy a ciele
	N.5.4	Narušenie dôveryhodnosti a dobrého mena štátu

Príloha č. 5 – Vzorové časti oblastí analýzy rizík

Oblasť 2 – Správa zraniteľností a kybernetických hrozieb

Existujúce bezpečnostné opatrenia:

- **E.2.1 –** v prípade výskytu zraniteľnosti prebieha v zmysle SLA zmluvy medzi dodávateľom a prevádzkovateľom systému komunikácia ohľadne hľadania spôsobov jej pokrytia, tieto sa ošetrujú na základe vzájomnej dohody
- **E.2.2 –** v prostredí prevádzkovateľa IS sa aktualizácia serverov s OS Windows uskutočňuje 2x za rok. Existuje proces update managementu, je definovaná všeobecná šablóna, ktorá obsahuje informácie o konkrétnych aktualizáciách (napr. koho kontaktovať, kto testuje, nasadzuje aktualizácie)
- **E.2.3 –** v prípade zistenia zraniteľnosti na danej platforme posiela správca danej platformy všetkým dotknutým IS, ktoré sú na nej prevádzkované, potrebné informácie na pokrytie identifikovanej zraniteľnosti
- **E.2.4 –** ....

Analyzované scenáre rizík:

R.2.1 – Využívanie zastaraných a nepodporovaných softvérových komponentov

Z bezpečnostného hľadiska prináša prevádzka zastaraných a nepodporovaných komponentov viaceré problémy, ako je napr. ukončený vývoj a oprava chýb zo strany výrobcu, nemožnosť pokryť identifikovanú bezpečnostnú zraniteľnosť a v neposlednom rade predstavuje atraktívny cieľ potenciálnych útočníkov. Využívaný komponent X je zastaraný a nie je podporovaný výrobcom. V rámci ISVS sa využívajú aj ďalšie komponenty, ktoré sú neaktualizované (komponent Y), resp. bez podpory výrobcu (komponent Z). V rámci vulnerability assessmentu (realizovaného v mesiaci M 202X) boli identifikované ďalšie kritické zraniteľnosti (ako napr. zraniteľné verzie nástroja A, či zraniteľné verzie knižníc B, C). Hrozí zneužitie neošetrených bezpečnostných zraniteľností útočníkom, ktoré môžu mať za následok prienik útočníka do ISVS a vnútornej siete prevádzkovateľa IS a kompromitáciu jeho aktív.

Existujúce opatrenia:	E.2.1, E.2.2, E.2.3		
Pravdepodobnosť:	Vysoká	**Následok:** Závažný	**Riziko: Vysoké**
Navrhované opatrenia:	O.2.1, O.2.2, O.2.3		

R.2.2 – .....

.....

Existujúce opatrenia:	E.2.x, ...		
Pravdepodobnosť:		**Následok:**	**Riziko:**
Navrhované opatrenia:	O.2.X		

Navrhované bezpečnostné opatrenia:

Kritické:

- **O.2.1** – zastarané verzie komponentov a zraniteľnosti identifikované v rámci vulnerability assessmentu (realizovaného v mesiaci M 202X) náležite riadiť a zabezpečiť aktualizáciu daných komponentov
- **O.2.2** – využívaný komponent X nahradiť produktom, ktorý má zabezpečenú podporu od výrobcu, pre ďalšie produkty (napr. komponent Z) danú podporu zakúpiť
- **O.2...** –

Nekritické:

- **O.2.3** – realizovať pravidelné vyhodnotenie používaných komponentov, resp. častí zdrojového kódu z hľadiska ich zastarania a v prípade potreby v rámci rozvoja systému navrhnúť možnosti aktualizácie a nahradenia zastaraných komponentov bezpečnými alternatívami
- **O.2...** –

Oblasť 3 – Správa aktív a riadenie kybernetických hrozieb a rizík

Existujúce bezpečnostné opatrenia:

- **E.3.1** – základný rámec riadenia rizík je uvedený v stratégii kybernetickej bezpečnosti, konkrétne zásady sú uvedené v politike riadenia rizík informačnej a kybernetickej bezpečnosti č. X/2024
- **E.3.2** – čiastočne je analýza rizík prostredia prevádzkovateľa IS historicky posudzovaná v rámci bezpečnostných projektov vyvíjaných IS (komplexná analýza rizík prostredia prevádzkovateľa neexistuje). Aktuálne prebieha projekt zameraný na vykonanie analýzy bezpečnosti organizácie ako celku, vrátane vykonania analýzy rizík vybraných IS. Je plánované aj vytvorenie pracovnej skupiny, ktorej členovia budú mať v zodpovednosti riadenie rizík
- **E.3.3 –** ...
- **E.3.4 –** ....

Analyzované scenáre rizík:

R.3.1 – Nedostatočný systém riadenia rizík

Zavedenie systému riadenia rizík súvisiacich s informačnou a kybernetickou bezpečnosťou vychádza z legislatívnych požiadaviek (najmä zákona o KB, zákona o ITVS), jeho nedostatočné definovanie a implementácia môže spôsobiť, že závažné riziká nebudú dostatočne riadené či včas identifikované. Zároveň môže dôjsť k nedostatočnému posúdeniu stavu konkrétnych rizík, dôsledkom čoho môžu byť nevhodne nastavené bezpečnostné opatrenia, ktoré majú dané riziká minimalizovať na akceptovateľnú úroveň. V prostredí prevádzkovateľa IS systém riadenia rizík v praxi nie je vhodne implementovaný, riziká nie sú riadené koncepčne, ostávajú dlhodobo nepokryté. Bezpečnostné opatrenia určené na ich elimináciu nie sú často implementované. Komplexná vrcholová analýza rizík celého IT prostredia nebola realizovaná, pravidelné preskúmavanie rizík sa nerealizuje. Metodika analýzy rizík nie je v interných predpisoch definovaná. Bezpečnostné opatrenia z bezpečnostných projektov či auditov bezpečnosti nie sú historicky vhodne riadené, sledované a vyhodnocované.

Existujúce opatrenia: E.3.1, E.3.2

Pravdepodobnosť:	Veľmi vysoká	**Následok:** Závažný	**Riziko: Veľmi vysoké**
Navrhované opatrenia:	O.3.1, O.3.2, O.3.3		

R.3.2 –			
.....			
Existujúce opatrenia:	E.3.x, ...		
Pravdepodobnosť:		**Následok:**	**Riziko:**
Navrhované opatrenia:	O.3.X		

Navrhované bezpečnostné opatrenia:

Kritické:

- **O.3.1** – procesy súvisiace s riadením a analýzou rizík informačnej a kybernetickej bezpečnosti definované v interných predpisoch implementovať do praxe, zahrnúť do interných predpisov aj metodiku analýzy rizík
- **O.3.2** – riziká identifikované v tejto analýze bezpečnosti začleniť do celkového systému riadenia rizík a zabezpečiť implementáciu súvisiacich navrhovaných opatrení v praxi
- **O.3...** –

Nekritické:

- **O.3.3** – dôsledne zvážiť každé schválenie výnimky neimplementovaných bezpečnostných opatrení a pristúpiť ku koncepčnému riešeniu informačnej a kybernetickej bezpečnosti v prostredí prevádzkovateľa IS
- **O.3...** –

Oblasť 5 – Riadenie kontinuity činností, zálohovanie, obnova systémov po havárii a krízové riadenie

Existujúce bezpečnostné opatrenia:

- **E.5.1** – procesy súvisiace so zabezpečením dostupnosti sú uvedené v interných predpisoch prevádzkovateľa IS, podrobnosti súvisiace so zabezpečením dostupnosti IS sú uvedené v detailnom návrhu riešenia IS, v prevádzkovej dokumentácii IS a v havarijnom pláne IS

- **E.5.2** – v technickej špecifikácii IS sú uvedené informácie a postupy súvisiace so zálohovaním virtuálnych serverov, DB a aplikačných komponentov IS, ako aj všeobecný popis riešenia pre obnovu databázy a aplikácie IS
- **E.5.3** – aplikačné servery umiestnené v dátových centrách sú prevádzkované spôsobom active-active (obidve lokality môžu obsluhovať požiadavky súčasne v závislosti od konfigurácie), lokálny load balancer v primárnom dátovom centre vytvára zabezpečené prepojenie aj na záložné dátové centrum
- **E.5.4** – v prevádzkovej dokumentácii IS je uvedený spôsob monitorovania dostupnosti aplikačných modulov a OS, sú sledované parametre ako dostupnosť servera na sieťovej úrovni, dostupnosť systémových služieb, dokumentácia obsahuje aj zoznam serverov pre nastavenie monitorovania dostupnosti a udalostí OS
- **E.5.5 –** ...
- **E.5.6 –** ...

Analyzované scenáre rizík:

R.5.1 – Nemožnosť obnovy IS

Pri výskyte havarijného stavu môže dôjsť k poškodeniu aplikačných údajov IS, k narušeniu konfigurácie IS a nemožnosti ich obnovy do pôvodného stavu. Pre rýchlu a konzistentnú obnovu činnosti systému je nevyhnutná existencia dostatočných postupov obnovy, záznamov o konfigurácii systému a záložných zdrojov údajov, z ktorých sa systém dá obnoviť. S uvedenými okolnosťami je nevyhnutné počítať už od začiatočných fáz projektu a návrhu systému, v opačnom prípade sa môžu vyskytnúť prípady neprimerane dlhej nedostupnosti systému či strata možnosti obnovy.

Existujúce opatrenia: E.5.1, E.5.2, E.5.3, E.5.4

Pravdepodobnosť: Stredná **Následok:** Stredný **Riziko: Stredné**

Navrhované opatrenia: O.5.1, O.5.2

R.5.2 – .....

.....

Existujúce opatrenia: E.5.X, ...

Pravdepodobnosť: **Následok:** **Riziko:**

Navrhované opatrenia: O.5.X

Navrhované bezpečnostné opatrenia:

Kritické:

- **O.5...** –

Nekritické:

- **O.5.1 –** dostupnosť zdrojov potrebných pre riešenie havarijných stavov overovať v rámci pravidelného testovania havarijného plánu IS
- **O.5.2 –** zásadné rozhodnutia a prípadné výnimky pri riešení havarijného stavu IS vždy schvaľovať zo strany vedúceho havarijného tímu a zabezpečiť ich podrobné zdokumentovanie
- **O.5...** –

Príloha č. 6 – Vzorová sumarizačná tabuľka rizík a ich atribútov

Vzorová sumarizačná tabuľka rizík a ich atribútov je uvedená v samostatnom dokumente vo formáte MS Excel.