MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PROJEKTOVÝ ZÁMER

Vzor pre manažérsky výstup I-02

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	Mesto Banská Bystrica
Názov projektu	Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica
Zodpovedná osoba za projekt	Ing. Beáta Galková
Realizátor projektu	Mesto Banská Bystrica
Vlastník projektu	Ing. Bibiána Palušková

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Ing. Bibiána Palušková	Mesto Banská Bystrica	Manažér kybernetickej bezpečnosti	20.04.2024	

Obsah

1. HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Meno
0.1	03.04.2024	Draft pracovnej verzie	Ing. Bibiána Palušková
0.2	20.04.2024	Zapracované pripomienky z v 0.1	Ing. Bibiána Palušková
1.0	26.4.2024	Predložené na schválenie	Ing. Bibiána Palušková

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s **Vyhláškou Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy** je dokument I-02 Projektový zámer určený na rozpracovanie podrobných podporných informácií prípravy projektu, aby bolo možné rozhodnúť o pokračovaní prípravy, projektu, pláne realizácie, alokovaní rozpočtu a ľudských zdrojov.

Dokument Projektový zámer v zmysle vyššie uvedenej vyhlášky obsahuje manažérske zhrnutie, rozsah, ciele a motiváciu Povinnej osoby (ďalej len Mesto alebo Mesto Banská Bystrica alebo Objednávateľ) realizovať projekt. Dokument zároveň uvádza informácie o zainteresovaných stranách, prístup k známym alternatívam smerovania a riadenia projektu, návrh merateľných ukazovateľov s ohľadom na schému uvažovaného financovania, podrobný popis požadovaných projektových výstupov ako aj obmedzení projektu, projektový predpokladov a tolerancií ako aj návrh organizačného zabezpečenia projektu.

Súčasťou predkladaného Projektového zámeru je detailný opis rozpočtu projektu a prínosov projektu v kontexte odhadovaných projektových nákladov, náhľad relevantných domén architektúr, ak ich realizácia projektu ovplyvňuje ich zmenu ako aj plánovaný časový harmonogram projektu s väzbami na plánované aktivity a výstupy projektu v súlade s konvenciou riadenia projektov PRINCE2.

2.1 Použité skratky a pojmy

SKRATKA	POPIS
TBD	To Be Determined (ešte určiť)
IB	Informačná bezpečnosť
KB	Kybernetická bezpečnosť
ITVS	Informačné technológie a výpočtové systémy
IKT	Informačné a komunikačné technológie
AR/BIA	Analýza rizík/Business Impact Analysis
HW	Hardvér (hardware)
SW	Softvér (software)
IS	Informačný systém
BCM	Business Continuity Management
DRP	Disaster Recovery Plan
OTP	One-Time Password
IT	Informačné technológie
IEEE 802.1X	Štandard pre kontrolu prístupu do siete
CAPEX	Kapitálové výdavky (Capital Expenditure)
OPEX	Prevádzkové výdavky (Operating Expenditure)

2.2 Konvencie pre typy požiadaviek (príklady)

Užívateľské požiadavky majú nasledovnú konvenciu:

U_nn_Rxx

- U – užívateľská požiadavka
- Nn – typ používateľa
- R – označenie požiadavky
- Xx – číslo požiadavky

Procesné požiadavky majú nasledovnú konvenciu:

P_ABXY_Rxx

- P - procesná požiadavka
- AB – označenie procesu
- XY – číslo podprocesu
- R – označenie požiadavky
- Xx – číslo požiadavky

Požiadavky na reporting majú nasledovnú konvenciu:

R_ABXY_Rxx

- R – požiadavka na reporting
- Nn – číslo reportu
- R – označenie požiadavky
- Xx – číslo požiadavky

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Jedným zo strategických cieľov Koncepcie kybernetickej bezpečnosti schválenej v roku 2015 vládou Slovenskej republiky je otvorený, bezpečný a chránený kybernetický priestor, ktorý zabezpečí vybudovanie dôvery v spoľahlivosť a bezpečnosť štátu a to najmä kritickej infraštruktúry a komunikačnej infraštruktúry, ako aj istoty, že tieto budú plniť svoje funkcie a slúžiť národným záujmom. Na druhej strane situácia v oblasti informačnej a kybernetickej bezpečnosti vo verenej správe nie je v ideálnom stave a kondícii. Väčšina orgánov verejnej správy nemá implementované riešenia a opatrenia kybernetickej bezpečnosti povinné podľa zákona o KB a zákona o ITVS. Z externého pohľadu sa zvyšuje frekvencia a závažnosť útokov z externého prostredia a na druhej strane sa zvyšuje závislosť orgánov verejnej správy na informačných aktívach a informačných systémoch, na ktorých je činnosť orgánov verejnej správy neodbytne závislá. Zvyšujú sa teda hrozby, zraniteľnosti a následne aj možné dopady bezpečnostných incidentov. Projektový zámer vychádza z horeuvedenej koncepcie ako aj strategických cieľov **Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025**[1], ktorá definuje strategické ciele Slovenskej republiky v oblasti kybernetickej a informačnej bezpečnosti. Tento strategický dokument v bode 4.4 definuje kybernetickú bezpečnosť (ďalej ako „KB“) ako základnú súčasť verejnej správy: ***„V kybernetickom priestore musia dobre fungovať nielen služby súkromných spoločností, ale aj tie poskytované štátom“.*** *Služby, ktoré ponúka svojim občanom musia byť dostatočne zabezpečené, aby nedošlo k zneužitiu citlivých alebo osobných údajov v kontexte Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679“.* Mesto Banská Bystrica ako Povinná osoba a iniciátor tohto projektového zámeru si plne uvedomuje, že súčasné kybernetické hrozby v kontexte svetových udalostí nie sú len hrozbami fiktívnymi, ale predstavujú skutočné riziko, ktoré ohrozuje informačné aktíva v jeho gescii a prevádzke ako prevádzkovateľa základnej služby. Mesto Banská Bystrica má v oblasti IKT dlhodobo víziu napĺňať ciele Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025, ako aj zodpovedne pristupovať k zabezpečeniu a riadeniu svojich informačných aktív prostredníctvom uplatňovania systematického prístupu ku kybernetickej a informačnej bezpečnosti založenej na analýze a riadení rizík, prostredníctvom poskytovania bezpečných a dostupných elektronických služieb mesta ako subjektu verejnej správy pre všetkých svojich občanov, podnikateľov ako aj návštevníkov. **Motiváciou Mesta Banská Bystrica predložiť tento projektový zámer a realizovať projekt je reflektovať na známe zistenia z už vykonaných auditov KB realizovaných v jeho prostredí, tak, aby projekt v čo najväčšej miere prispel k zosúladeniu oblasti riadenia kybernetickej a informačnej bezpečnosti s požiadavkami a očakávaniami príslušných štátnych orgánov ako aj príslušných aktuálne platných legislatívnych požiadaviek.** Mesto Banská Bystrica sa napriek identifikovaným viacerým potrebným opatreniam v oblasti zabezpečenia informačnej a kybernetickej bezpečnosti rozhodlo pre zameranie sa na opatrenia, ktoré predstavujú najvyššiu mieru rizika a najvyššie možné dopady v kontexte súčasne identifikovaného nesúladu s legislatívnymi požiadavkami, ktoré vyplývajú z ostatne vykonaného auditu kybernetickej bezpečnosti. Rozsah projektového zámeru súčasne vychádza z vykonanej viacfaktorovej analýzy možných alternatív ako variantných riešení a teda navrhované riešenie ako optimálne je vytvorené na základe predošlej uskutočnenej dôslednej selekcie.

Mesto Banská Bystrica si uvedomuje, že vývoj v oblasti informačných a komunikačných technológií, narastajúca komplexnosť, diferencovanosť, technologická rozmanitosť súčasne zvyšujú rozsah perimetra pre vykonanie kybernetického útoku, ktorých prípadné vykonanie by ohrozilo riziko dôvery Mesta Banská Bystrica u používateľov poskytovanej základnej služby. Z tohto dôvodu Mesto Banská Bystrica považuje za nevyhnutné prijímať a realizovať opatrenia na ochranu svojich informačných aktív vrátane zabezpečenia informácií, ktoré sú vo veľkej miere v rámci implementácie efektívnej verejnej správy (teda aj v oblasti miestnej samosprávy) poskytované, ukladané

[1] https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf

a vymieňané v kybernetickom priestore. Zavedením správnych opatrení je možné minimalizovať riziká, ktoré kybernetický priestor pre Mesto Banská Bystrica prináša a to hlavne:

- Odcudzenie, zneužitie alebo strata dôvernosti a/alebo dostupnosti osobných a inak citlivých údajov;
- Poškodenie reputácie Mesta Banská Bystrica ako poskytovateľa základnej služby a služieb pre občanov;
- Znefunkčnenie poskytovaných elektronických služieb pre občanov mesta.

Mesto Banská Bystrica definuje tento Projektový zámer nie len s ohľadom na prístup štátu v oblasti zabezpečenia informačnej a kybernetickej bezpečnosti, ale aj s ohľadom na vlastné potreby, ktoré boli identifikované na základe zistení a odporúčaní ostatne vykonaného auditu kybernetickej a informačnej bezpečnosti, ktorý bol vykonaný v súlade s § 29 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej „Zákon o KB“)[2]. V súlade s § 20 Zákona o KB je Mesto Banská Bystrica povinné plniť predmetné opatrenia, ktorými bude zabezpečovať pokrytie významných aspektov kybernetickej bezpečnosti, ktoré majú vplyv na celú organizáciu. **Cieľom projektu je zaistenie kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB.** Vzhľadom na šírku oblastí bezpečnostných opatrení ako aj na technické, administratívne a finančné kapacity Mesta Banská Bystrica boli ciele projektu identifikované s dôrazom na ich čo najväčší efekt a predpokladaný pozitívny dopad na oblasť informačnej a kybernetickej bezpečnosti organizácie, ktorá je prevádzkovateľom základnej služby. K prioritizácii riešených oblastí Mesto Banská Bystrica dospelo na základe ostatne vykonaného auditu kybernetickej a informačnej bezpečnosti ako aj potreby vykonania opakovaného auditu informačnej a kybernetickej bezpečnosti. V rámci projektu má Mesto Banská Bystrica zámer realizovať nasledovné opatrenia na zvýšenie úrovne informačnej a kybernetickej bezpečnosti, ktoré prispejú k celkovému zlepšeniu technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti kybernetickej a informačnej bezpečnosti v jeho prostredí:

1. Vykonať opakovaný audit informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB;
2. Vypracovať relevantnú bezpečnostnú dokumentáciu;
3. Implementovať a konfigurovať systém pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica;
4. Vykonať segmentáciu siete Mesta Banská Bystrica s ohľadom na súčasné prevádzkové požiadavky;
5. Zrealizovať výmenu aktívnych prvkov core časti siete;
6. Implementovať systém dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete;
7. Implementovať riešenie centrálneho bezpečnostného manažmentu pre koncové stanice;

V rámci jednotlivých aktivít Mesto plánuje vykonať školenie dotknutého personálu na implementované technológie a riešenia, tak aby bola zabezpečená kontinuita business procesov ako aj udržateľnosť projektu 60 kalendárnych mesiacov po ukončení jeho realizačnej fázy.

Motívom realizácie horeuvedených opatrení sú okrem uvedeného aj nasledovné dôvody:

- Potreba odbúravania agendy a odľahčenie nedostatočných personálnych kapacít pre oblasť riadenia IB a KB na prevádzku bezpečnostných systémov;
- Absencia realizácie základnej analýzy rizík a analýzy dopadov (AR/BIA);
- Absencia uceleného konceptu riadenia rizík a absencia spracovania základných dokumentov v oblasti KB a IB a akvizície HW a SW komponentov v súlade so Zákonom o KB.

Realizácia vyššie uvedených opatrení prispeje k celkovému zvýšeniu úrovne informačnej bezpečnosti a kybernetickej bezpečnosti ako aj k odstraňovaniu zistení a nesúladov identifikovaných v ostatne vykonanom audite kybernetickej a informačnej bezpečnosti, čo jednoznačným spôsobom reflektuje zámer Mesta Banská Bystrica alokovať svoje zdroje a kapacity na oblasti informačnej a kybernetickej bezpečnosti, v rámci ktorých sú objektívne identifikované najvyššie miery rizika, potenciálny dopad a najvyššia miera nesúladu s legislatívnymi požiadavkami.

Iniciatíva projektu a zdôvodnenie projekt realizovať zároveň vychádza z viacerých vzájomne previazaných predpokladov a potrieb:

- Nárast rizika kybernetických útokov zameraných na subjekty verejnej správy a prevádzkovateľov základnej služby;
- Potreba zvýšenia efektivity procesov riadenia informačnej a kybernetickej bezpečnosti rámci IKT organizácie;
- Potreba riešenia nedostatku kvalifikovaných odborných IKT špecialistov a špecialistov informačnej bezpečnosti a kybernetickej bezpečnosti prostredníctvom centrálnej správy, automatizácie a manažmentu procesov a aktív;
- Potreba zvýšenia transparentnosti a efektívnosti manažmentu výkonu prevádzky IKT v organizácii;
- Potreba zvýšenia visibility v monitorovaných IS prostredníctvom implementácie manažmentových a dohľadových nástrojov;
- Naplnenie zákonných a regulatívnych požiadaviek;
- Zvýšiť bezpečnosť siete prostredníctvom rozšírenia prístupových pravidiel pri zachovaní užívateľského komfortu;
- Absencia vykonania inventarizácie informačných aktív, vykonania klasifikácie a kategorizácie IS a sietí, vykonania AR a BIA ako aj absencia zabezpečenia formalizovaného a opakovaného procesu riadenia identifikovaných rizík (ich mitigácie), ktoré sú nevyhnutným a nutným predpokladom pre efektívne riadenie rizík IB a KB;
- Absencia bezpečnostných opatrení pre jednotlivé klasifikačné stupne a kategórie IS a absencia základnej sady dokumentácie požadovanej Zákonom o KB;
- Absencia základných smerníc pre výkon procesov riadenia IB a KB v rámci jednotlivých oblastí riadenia;
- Absencia ľudských kapacít na efektívny bezpečnostný monitoring, konsolidáciu logov a auditných záznamov, analýzu bezpečnostných udalostí a incidentov a aj na ich riešenie so súčasnou snahou odbúrania pracovnej záťaže prechodom na automatizáciu a digitalizáciu týchto procesov.

Navrhované opatrenia predstavujú vzhľadom na aktuálny stav IB a KB Mesta Banská Bystrica nutný základ pre zefektívnenie riadenia IB a KB ako aj základ pre implementáciu dodatočných opatrení a technických bezpečnostných riešení. Výstupy týchto opatrení možno vnímať ako nevyhnutný predpoklad pre prijímanie adekvátnych, efektívnych, vyvážených a optimálnych bezpečnostných opatrení. Mesto Banská Bystrica realizáciou projektu zároveň očakáva, že okrem samotného zvýšenia úrovne IB a KB vytvorí dostatočný základ v oblasti governance ako aj v oblasti technických opatrení, ktorý mu umožní aj v budúcnosti nadväzovať na aktivity tohto projektu tak, aby mesto mohlo získavať opakovane externé zdroje pre kontinuálny a koncepčný rozvoj v oblasti IB a KB, nakoľko túto situáciu

[2] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/

nevníma ako statickú entitu ale ako dynamický, neustále sa rozvíjajúci a živý proces, ktorý odráža zaužívané princípy efektívneho riadenia IKT aktív so zameraním sa na kontinuálne zlepšovanie.

Realizácia horeuvedených opatrení bude zároveň podporená školeniami dotknutých stakeholderov tak, aby prechod na novo implementované riešenia a obstarané HW a SW komponenty bol plynulý a bola zabezpečená kontinuita prevádzky služieb poskytovaných pred realizáciou projektu. Ciele projektu korešpondujú s víziou Mesta Banská Bystrica byť **odolným, inovatívnym a inteligentným, bezpečným mestom**[3]**,** a teda rozvíjať bezpečnosť vo všetkých oblastiach života mesta vrátane informačnej a kybernetickej bezpečnosti (súlad s navrhovaným špecifickým cieľom **8.1.2 Rozvíjať bezpečnosť vo všetkých oblastiach života mesta.**

Očakávané prínosy projektu:

- Aktualizácia overenia plnenia povinností podľa Zákona o KB spolu s posúdením zhody prijatých bezpečnostných opatrení s požiadavkami podľa Zákona o KB, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby;
- Preverenie účinnosti doposiaľ prijatých bezpečnostných opatrení a odpočet plnenia požiadaviek stanovených Zákonom o KB;
- Zavedenie systému pre zabezpečenie siete a správu identít a zabezpečenie prístupov do siete a k aktívam v siete;
- Zvýšenie úrovne zabezpečenia siete, jej výkonnosti, správy ako aj ochrany vykonaním segmentácie siete;
- Zvýšenie úrovne a rozsahu centralizovanej správy a sledovania siete, rozšírenie rozsahu nástrojov na diagnostiku a analýzu a zabezpečenie pokročilejších bezpečnostných funkcií prostredníctvom výmeny zastaralých, end-of-support a end-of-sales aktívnych sieťových prvkov;
- Zvýšenie bezpečnosti pri prístupe k aktívam, zníženie rizika zneužitia hesiel, zvýšenie ochrany citlivých údajov a dodatočné zvýšenie úrovne zabezpečenia prístupu do siete zavedením dvojfaktorovej autentifikácie.

Podrobnejší opis opatrení (aktivít projektu):

Všetky aktivity projektu má Mesto Banská Bystrica záujem financovať prostredníctvom kombinácie zdrojov EÚ, národných zdrojov a vlastných zdrojov v rámci aktuálne vyhlásenej Výzvy „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejná správa“, kód výzvy PSK-MIRRI-611-2024-DV-EFRR, (ďalej len „Výzva“) v súlade s možnou mierou intenzity spolufinancovania uvedenou v časti 4 Výzvy. V prípade nezískania prostriedkov, nebude možné pristúpiť k realizácií optimálneho variantného riešenia.

1. Vykonanie opakovaného auditu informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB

Zámerom tejto aktivity je vykonanie pravidelne opakujúceho sa auditu IB a KB v súlade s § 29 Zákona o KB. Mesto Banská Bystrica v čase kreovania tohto projektového zámeru má plán realizovať audit s už jestvujúcim zmluvným partnerom. Vzhľadom na skutočnosť, že zahájenie opakovaného auditu pripadá na obdobie, ktoré časovo pripadá dátumu po vyhlásení Výzvy, Mesto Banská Bystrica má v pláne využiť možnosť financovať náklady vzniknuté po tomto období, čo rozsahovo zodpovedá celému auditu, ktorý sa plánuje realizovať. Aktivita bude pozostávať z preplatenia nákladov spojených s činnosťou špecialistov z oblasti IB a KB podieľajúcich sa na výkone opakovaného auditu. Indikatívna výška prostriedkov ako aj časový horizont realizácie tejto aktivity sú uvedené v časti „Rozpočet a prínosy“ a „Harmonogram jednotlivých fáz a metóda jeho riadenia“.

Väzba na oprávnenú aktivitu z Výzvy: O.2) Audit a kontrolné činnosti – Obstaranie prvého alebo opakovaného auditu kybernetickej bezpečnosti v súlade so zákonom o KB.

2. Vypracovanie relevantnej bezpečnostnej dokumentácie

Mesto Banská Bystrica momentálne nedisponuje žiadnou z povinnej dokumentácie v zmysle Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných opatrení v znení vyhlášky č. 264/2023 Z. z. Z tohto dôvodu je jednou z hlavných priorít v rámci uvažovaného projektu zabezpečiť dopracovanie relevantnej dokumentácie a zosúladenie so zákonnými požiadavkami kladenými na poskytovateľa základnej služby. V súčasnosti Mesto Banská Bystrica disponuje iba zriadeným bezpečnostným výborom, ale samotné riadenie IB a KB nie je formalizované. Predmetom tejto aktivity sú nasledovné činnosti a vypracovanie nasledovnej bezpečnostnej dokumentácie zohľadňujúcej aktuálny stav a potreby Mesta:

- Vykonanie inventarizácie aktív vrátane klasifikácie informácií a kategorizácie sietí a informačných systémov;
- Vypracovanie analýzy rizík (AR) podľa požiadaviek uvedených v Zákone o KB;
- Vypracovanie analýzy dopadov a kľúčových procesov a činností (BIA) vrátane prípravy smernice/metodiky pre riadenie oblasti BCM, prípravy plánov BCM a plánov obnovy DRP.
- Vypracovanie základných bezpečnostných politík KB:
    - Bezpečnostná stratégia kybernetickej bezpečnosti;
    - Politika organizácie bezpečnosti;
    - Politika pre riadenie bezpečnosti rizík;
    - Politika pre riadenie informačných aktív;
    - Pravidlá správania a dobrej praxe;
    - Politika pre riadenie dodávateľských vzťahov;
    - Politika pre riadenie vývoja a údržby v oblasti IKT;
    - Politika pre riadenie a prevádzku IKT;
    - Politika pre riadenie súladu;
    - Politika pre riadenie kontinuity procesov a činností.

Aktivita bude pozostávať z poskytnutia služieb – činností expertov v oblasti IB a KB. Indikatívna výška prostriedkov ako aj časový horizont realizácie tejto aktivity sú uvedené v časti „Rozpočet a prínosy“ a „Harmonogram jednotlivých fáz a metóda jeho riadenia“.

Väzba na oprávnené aktivity z Výzvy: A.1) Organizácia KIB – Vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení.

[3] https://tvormespolu.banskabystrica.sk/processes/programrozvojamesta

3. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica

Mesto Banská Bystrica momentálne rieši prístup do siete iba na úrovni prihlasovacie meno + heslo v rámci užívateľov vytvorených v rámci Active Directory. V súčasnom stave je možné sa však v rámci vnútornej siete pripojiť prostredníctvom akéhokoľvek zariadenia, keďže nejestvujú žiadne politiky a nástroje, ktoré by umožňovali definovať rozsah/typy/skupiny zariadení, ktorých prístup do siete je povolený.

Táto situácia predstavuje značné riziko vzniku kybernetického incidentu, keďže prevádzka a správa IKT Mesta nemá možnosti a nástroje ako takýmto prístupom efektívne zabrániť. Zámerom v rámci tejto aktivity je obstarať a nasadiť SW riešenie, pomocou ktorého bude možné vykonávať centralizovanú autentifikáciu a autorizáciu pre rôzne typy používateľov a zariadení v sieti, spravovať politiky prístupu na základe definovania identít, rolí, zariadení, prípadne ďalších správcom siete voliteľných atribútov, sledovať a revidovať prístupy používateľov do siete, spravovať prístupy do siete zariadeniami pristupujúcimi v režime BYOD („Bring Your Own Device“) – zariadení, ktoré nie sú v správe a priamej kontrole správcu IKT Mesta. Implementácia takéhoto riešenia zjednotí, zjednoduší a urýchli správu prístupov v rámci siete Mesta Banská Bystrica. Nasadené riešenie bude súčasne podporovať štandard IEEE 802.1X pre autentifikáciu a autorizáciu zariadení, ktoré budú nadväzovať spojenie so sieťou Mesta. Riešenie bude zabezpečovať kontrolu prístupu do siete na úrovni portov na aktívnych sieťových prvkoch. Pre účely plnohodnotného nasadenia overovania na úrovni celej siete organizácie bude potrebné realizovať výmenu sieťových prvkov, ktoré sú „end-of-sales“ a „end-of-support“ a súčasne nepodporujú protokol 802.1X. Z tohto dôvodu je zámerom Mesta Banská Bystrica realizovať nákup nových aktívnych sieťových prvkov, ktoré budú súčasťou implementovaného riešenia v celkovom počte 7 ks.

Aktivita bude pozostávať z obstarania SW riešenia pre centrálnu správu prístupov / identít ako aj obstarania HW komponentov, ktoré podporujú protokol IEEE 802.1X. Indikatívna výška prostriedkov ako aj časový horizont realizácie tejto aktivity sú uvedené v časti „Rozpočet a prínosy“ a „Harmonogram jednotlivých fáz a metóda jeho riadenia“.

Väzba na oprávnené aktivity z Výzvy: D.2) Riadenie prístupov – Zavedenie, implementácia alebo aktualizácia centrálneho nástroja na správu a overovanie identity, nástroja na riadenie prístupových oprávnení vrátane prístupových práv a kontroly prístupových účtov a prístupových oprávnení.

4. Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky

Potreba realizácie segmentácie siete úzko súvisí s aktivitou č.3, nakoľko výstupy aktivity č.3 bude súčasne nevyhnutne potrebné koordinovať v kontexte logického členenia siete na segmenty zohľadňujúce prevádzkové a bezpečnostné požiadavky mesta. V súčasnosti Mesto Banská Bystrica nemá vykonanú komplexnú segmentáciu siete. V rámci projektu sa plánuje vykonať segmentácia siete súčasne s implementáciou a nasadením overovania podľa protokolu 802.1X. Realizácia segmentácie siete na logické celky v závislosti od súčasnej prevádzky, typov podsietí ako aj pristupujúcich používateľov a zariadení umožní rozdeliť sieť na VLAN, kde bude súčasne aplikovaná politika prístupov 802.1X, čo umožní lepšiu kontrolu prístupu na úrovni jednotlivých segmentov a to tak, že zariadenia bude možné pripojiť iba k segmentom, ktoré budú pre ne určené na základe ich identít a udelených prístupových práv/prístupových profilov. Kombináciou overovania prostredníctvom 802.1X a vykonaním segmentácie siete sa očakáva zvýšenie celkovej bezpečnosti siete, nakoľko možnosť použitia autentifikácie na každom segmente zabezpečí, že budú mať oprávnené zariadenia prístup iba do určitej časti siete, čo bude značným spôsobom minimalizovať riziko neoprávneného prístupu alebo pohybu zariadení v sieti. Implementáciou overovania 802.1X v kombinácií s vykonanou segmentáciou siete sa zároveň zabezpečí, že prípadné bezpečnostné incidenty a hrozby budú izolované na konkrétne menšie segmenty siete a identifikované problémové zariadenie nebude mať dopad na celú sieť ale len na konkrétny segment. Takéto nasadenie zároveň umožní dynamickú autentifikáciu zariadení a prístupov z pohľadu administrátora, ktorý bude môcť meniť prístupové pravidlá na úrovni portu ktoréhokoľvek segmentu.

Aktivita bude pozostávať z obstarania služieb činností expertov na sieťové a bezpečnostné technológie, ktorí vykonajú analýzu súčasného stavu, navrhnú optimálny budúci stav a zaistia vykonanie samotnej segmentácie siete v kontexte implementovaného overovania podľa 802.1X a obstaraných ako aj jestvujúcich aktívnych prvkov siete.

Väzba na oprávnené aktivity z Výzvy: I.1) Sieťová a komunikačná bezpečnosť – Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečnostného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel.

5. Výmena aktívnych prvkov CORE časti siete

Vzhľadom na skutočnosť, že podstatná časť CORE siete Mesta Banská Bystrica pozostáva z prevádzkovaných end-of-sale a end-of-support zariadení a zároveň sa neustále navyšujú potreby zvyšovania prenosovej rýchlosti a kapacity siete, Mesto Banská Bystrica potrebuje zabezpečiť výmenu vybraných aktívnych sieťových prvkov CORE časti siete, tak aby bola kontinuálne zachovaná vysoká úroveň bezpečnosti prevádzky siete prostredníctvom zachovania aktuálnych bezpečnostných funkcií zariadení aj vo vzťahu k aktuálne známym zraniteľnostiam a hrozbám od čoho sa očakáva zvýšenie celkovej úrovne zabezpečenia ochrany siete proti rôznym typom útokov. Vzhľadom na narastajúci počet aplikácií a systémov, ktoré Mesto Banská Bystrica spravuje, ako aj počet generovaných eventov v siete resp. requestov voči aplikáciám, ku ktorým pristupujú interní používatelia ako aj externí používatelia je potrebné zachovať vysokú úroveň dostupnosti všetkých prevádzkovaných IS Mesta. Výmenou potrebných aktívnych prvkov CORE časti siete Mesto Banská Bystrica zabezpečí kontinuálne požadovanú úroveň dostupnosti IT aktív a ich primeranú dobu odozvy. Výmena aktívnych prvkov v CORE časti siete je nevyhnutne potrebná aj vzhľadom na zámer vykonať segmentáciu siete Mesta ako aj implementovať systém pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica prostredníctvom protokolu IEEE 802.1X. Súčasný set dostupných sieťových prvkov neumožňuje plnohodnotné nasadenie tohto bezpečnostného protokolu, čo v praxi znamená, že by nebolo možné v rámci realizácie vyššie uvedených aktivít vykonať túto implementáciu cez všetky dotknuté oddelenia v sieti mestského úradu, na úrovni všetkých novo definovaných sieťových segmentov, čo by v podstate malo za následok, že efekt implementácie IEEE 802.1X s vykonaním segmentácie by mal len minimálny pozitívny dopad na organizáciu ako celok.

Aktivita bude pozostávať z obstarania aktívnych prvkov pre CORE časť siete, ktoré budú funkčne a výkonnostne zodpovedať požiadavkám na „TO-BE“ stav nie len z ohľadom na celkový performance siete, ale aj s ohľadom na vysoké štandardy bezpečnosti siete.

Celkovo sa očakáva obstaranie 9 ks aktívnych prvkov pre CORE časť siete súčasne s vykonaním revízie konfigurácie a implementácie nových konfiguračných pravidiel vrátane pravidiel na firewalloch. Indikatívna výška prostriedkov ako aj časový horizont realizácie tejto aktivity sú uvedené v časti „Rozpočet a prínosy“ a „Harmonogram jednotlivých fáz a metóda jeho riadenia“.

Väzba na oprávnené aktivity z Výzvy: Väzba na oprávnené aktivity z Výzvy: D.2) Riadenie prístupov – Zavedenie, implementácia alebo aktualizácia centrálneho nástroja na správu a overovanie identity, nástroja na riadenie prístupových oprávnení vrátane prístupových práv a kontroly prístupových účtov a prístupových oprávnení

a

I.1) Sieťová a komunikačná bezpečnosť – Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečnostného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel.

6. Implementácia systému dvojfaktorovej autentifikácie

Mesto v období 04/2024 realizuje opakovaný audit informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB. Z predbežných zistení vykonaného auditu ako aj z komunikácie s odborne spôsobilými osobami v oblasti vykonávania auditu bolo zistené, že jedným z najväčších nedostatkov úrovne zabezpečenia informačných aktív je nedostatočná vrstva ochrany pri overovaní identity používateľa pri prístupe do siete Mesta. Na základe uvedeného vyššie identifikovaného nedostatku sa Mesto Banská Bystrica snaží reflektovať na „AS-IS“ stav a zaviesť dvojfaktorové overovanie, kde okrem súčasného overovania prostredníctvom mena a hesla bude užívateľ nútený zadať generované heslo prostredníctvom SW tokenu a HW tokenu. Mesto Banská Bystrica v rámci zamýšľanej aktivity plánuje obstarať a implementovať systém dvojfaktorovej autentifikácie prostredníctvom obstarania SW / HW tokenov pre celkovo 700 používateľov. Riešenie bude realizované prostredníctvom HW/SW tokenu, ktorý bude generovať jednorazové heslá (OTP – One Time Passwords) pre používateľov prihlasujúcich sa do siete. Používateľ získa OTP prostredníctvom HW zariadenia a SW tokenu nainštalovaného na koncovej stanici. Riadenie identít dvojfaktorového overenia sa plánuje realizovať prostredníctvom platformy nasadenej na infraštruktúre dodávateľa, ktorý zabezpečí s ohľadom na konkrétnu implementáciu nevyhnutné výpočtové zdroje. Súčasťou dodávky bude integrácia dvojfaktorového overovania na jestvujúci systém pre správu identity.

Od implementácie dvojfaktorového overovania Mesto Banská Bystrica očakáva zvýšenie úrovne zabezpečenia prístupu do siete zabezpečením overovania nad rámec súčasného zadávania mena a hesla, keďže v súčasnosti útočníkovi na prístup do siete postačuje získať používateľské meno a heslo bez potreby zadania dynamicky meniaceho sa druhého prihlasovacieho faktoru ako aj zabezpečí súlad so zisteniami opakovaného auditu IB a KB realizovaného v roku 2024.

Aktivita bude pozostávať z obstarania riešenia dvojfaktorovej autentifikácie s celkovým počtom SW/HW tokenov pre 700 používateľov. V rámci aktivity bude vykonaná úvodná analýza, konfigurácia ako aj nasadenie v produkčnom prostredí.

Väzba na oprávnené aktivity z Výzvy: I.2) Sieťová a komunikačná bezpečnosť – Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a vzdialený prístup napríklad implementáciou dvojfaktorovej autentizácie alebo kryptografických prostriedkov.

7. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

Mesto Banská Bystrica momentálne nedisponuje uceleným riešením centrálneho manažmentu a dohľadu nad koncovými stanicami. To má za následok, že ochrana používateľských aktív nie je vzhľadom na rozsah perimetra siete s ohľadom na aktivity vykonávané užívateľmi dostatočná a preto má Mesto ambíciu zvýšiť úroveň zabezpečenia aj na úrovni koncových staníc, čo vníma ako doplňujúcu aktivitu k aktivitám týkajúcich sa výmeny aktívnych sieťových prvkov, riadenia prístupov ako aj segmentácie siete. Mesto vníma potrebu zabezpečiť zlepšenie v oblasti detekcie, investigácie a predikcie pred útokmi na koncové stanice. Z tejto potreby vyplýva potreba nasadenia riešenia, ktoré zabezpečí centrálnu správu ochrany koncových staníc, detekciu nevyžiadanej aktivity, funkcionalitu monitoringu prevádzky na koncovom zariadení a funkcionalitu možnosti centrálneho nastavovania bezpečnostných pravidiel na koncových staniciach. Realizácia tejto aktivity prispeje k holistickému zvýšeniu úrovne zabezpečenia informačných aktív Mesta. Okrem unifikácie a centralizácie zabezpečenia ochrany koncových zariadení aktivita prispeje k zjednodušeniu a systematizácii riadenia ochrany koncových staníc v prostredí Mesta.

Aktivita bude pozostávať z obstarania systému centrálneho dohľadu a manažmentu koncových zariadení pre minimálne 700 koncových staníc. V rámci aktivity bude vykonaná úvodná analýza, konfigurácia ako aj nasadenie v produkčnom prostredí.

Väzba na oprávnené aktivity z Výzvy: H.2) Ochrana proti škodlivému kódu – Implementácia alebo aktualizácia nástrojov na ochranu, ktoré okrem iného vykonávajú kontrolu prístupu k digitálnemu obsahu, pravidelné kontroly úložísk vrátane cloudových riešení, zabraňujú prístupu neoprávnených používateľom filtrovaním obsahu a zamedzením inštalovať alebo odinštalovať alebo zakázať funkcie systému na ochranu škodlivému kódu.

Školenie dotknutého personálu na implementované technológie.

Keďže projekt rieši pomerne širokú škálu činností, ktoré budú mať po úspešnom otestovaní a nasadení dopad na Stakeholderov (prevádzka IKT Mesta a/alebo používateľ koncového zariadenia) bude v rámci dodávok jednotlivých aktivít dodávateľ konkrétneho riešenia súčasne zodpovedný za vykonanie školenia, tak, aby používatelia vedeli výstupy projektu využívať v praxi počas výkonu bežnej agendy. V rámci projektu bude požadované, aby dodávatelia jednotlivých výstupov projektu zabezpečili nevyhnutný rozsah dokumentácie v zmysle Vyhlášky č. 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v rozsahu minimálnych požiadaviek na dokumentáciu a výstupy relevantné pre školenia.

3.2 Motivácia a rozsah projektu

V rámci Zákona o KB je stanovené, že identifikovaný prevádzkovateľ základnej služby plní požiadavky v nasledujúcom rozsahu:

§ 19 Povinnosti prevádzkovateľa základnej služby

- riešiť kybernetický bezpečnostný incident,
- bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
- spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,
- v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
- oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie

§ 20 Bezpečnostné opatrenia

Najmä pre oblasť:

- § 5 vyhlášky č. 362/2018 Z. z. organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
- § 6 vyhlášky č. 362/2018 Z. z. riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- § 7 vyhlášky č. 362/2018 Z. z. personálnej bezpečnosti,
- § 8 vyhlášky č. 362/2018 Z. z. riadenia prístupov,§ 9 vyhlášky č. 362/2018 Z. z. riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- § 10 vyhlášky č. 362/2018 Z .z. bezpečnosti pri prevádzke informačných systémov a sietí,
- § 11 vyhlášky č. 362/2018 Z. z. hodnotenia zraniteľností a bezpečnostných aktualizácií,
- § 12 vyhlášky č. 362/2018 Z. z. ochrany proti škodlivému kódu
- § 13 vyhlášky č. 362/2018 Z. z. sieťovej a komunikačnej bezpečnosti,
- § 14 vyhlášky č. 362/2018 Z. z. akvizície, vývoja a údržby informačných sietí a informačných systémov,
- § 15 vyhlášky č. 362/2018 Z. z. zaznamenávania udalostí a monitorovania,
- § 16 vyhlášky č. 362/2018 Z .z. fyzickej bezpečnosti a bezpečnosti prostredia,
- § 17 vyhlášky č. 362/2018 Z. z. riešenia kybernetických bezpečnostných incidentov,
- § 17a vyhlášky č. 362/2018 Z. z. kryptografických opatrení,
- § 17b vyhlášky č. 362/2018 Z. z. riadenia kontinuity prevádzky
- § 17c vyhlášky č. 362/2018 Z. z. auditu, riadenia súladu a kontrolných činností.

Na tieto požiadavky musí Mesto Banská Bystrica neustále reagovať tak, aby bol kontinuálne zabezpečovaný súlad s legislatívnymi požiadavkami. Práve uvedené vyššie je jedným z hlavných motivačných faktorov pre realizáciu uvažovaného projektu.

Motiváciou, prečo realizovať tento projekt je súčasne **celkové zlepšenie úrovne informačnej a kybernetickej bezpečnosti a to prostredníctvom aktivít, ktorých realizácia priamo reflektuje na krátko ako aj strednodobé zistenia a nedostatky v oblasti zabezpečenia informačných aktív Mesta Banská Bystrica ako prevádzkovateľa základnej služby.** Súčasným trendom je zvyšovanie objemu prenášaných údajov internou ale aj verejnou sieťou, nárast veľkosti perimetra siete Mesta, zvyšovanie počtu informačných aktív, či už sa jedná o informačné systémy alebo k nim podporné HW aktíva, čo sa prejavuje v zvyšovaní možností vykonania kybernetického útoku na infraštruktúru Mesta Banská Bystrica. Informačné systémy Mesta podliehajú neustálemu vývoju spojenému so zmenou, pričom frekvencia zmien má rovnako vzrastajúci trend, na čo Mesto Banská Bystrica musí pružne reagovať. Okrem vyššie uvedeného, aktíva Mesta interagujú s ďalšími systémami, ktoré sú z pohľadu Mesta v postavení externých systémov a služieb, či už na strane štátu alebo tretích strán z komerčného sektora. Aj nárast počtu integrácií a rozhraní s ktorými aktíva Mesta priamo alebo nepriamo interagujú vyvoláva zvýšenú potrebu nie len na bezpečnosť samotnú, ale aj dostupnosť a kvalitu poskytovaných ako aj konzumovaných služieb. Tento holistický pohľad na potrebu zabezpečenia vysokej úrovne kybernetickej i informačnej bezpečnosti aktív Mesta Banská Bystrica dáva za pre misiu Mesta poskytovať služby nie len bezpečné, ale aj kvalitné a dostupné.

Realizáciou navrhovaných aktivít projektu sa dosiahne vyriešenie nasledovných problémov:

1. Vykonanie opakovaného auditu informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB

- Splnenie legislatívnej požiadavky na pravidelný výkon auditu informačnej a kybernetickej bezpečnosti;
- Odpočet pôvodných zistení ako aj identifikácia nových zistení, na ktoré je potrebné reflektovať;
- Zvýšenie efektu realizácie navrhovaných aktivít v tomto Projektovom zámere prostredníctvom zohľadnenia výstupov auditu – podpora prioritizácie oblastí zamerania sa projektu s ohľadom na dostupné technické / personálne / finančné kapacity Mesta.
- Získanie uceleného aktuálneho prehľadu o stave zabezpečenia IB a KB.

2. Vypracovanie relevantnej bezpečnostnej dokumentácie

- Zlepšenie transparentnosti a bezpečnostných postupov Mesta ako organizácie v oblasti postupov, politík a procesov v oblasti IB a KB;
- Zníženie rizík a ochrana pred hrozbami vplyvom minimalizácie rizika úniku citlivých údajov, ktoré sú zberané, vytvárané, spracúvané, uchovávané, zdieľané v rámci informačných aktív Mesta;
- Zlepšenie konzistencie a súlad s legislatívou, zabezpečenie konzistentnosti v návrhu, organizácii a implementácii procesov a bezpečnostných politík a tým zameranie sa na dodržiavanie predpisov a štandardov v oblasti IB a KB.
- Zlepšenie procesu riadenia rizík vďaka identifikovaným a vyhodnoteným rizikám, ktorým Mesto Banská Bystrica čelí.

- Jasne a jednoznačne zadefinované interné postupy, smernice a stratégie, ktoré zohľadňujú aktuálny stav zabezpečenia informačných aktív Mesta ako aj súčasné legislatívne požiadavky kladené na Mesto ako prevádzkovateľa základnej služby;
- Zníženie pravdepodobnosti vzniku bezpečnostných incidentov vďaka implementácii definovaných postupov a opatrení uvedených vo vypracovanej bezpečnostnej dokumentácii;
- Zvýšenie celkovej úrovne zabezpečenia Mesta Banská Bystrica prostredníctvom vykonanej identifikácie a analýzy potenciálnych bezpečnostných hrozieb a zraniteľností v informačných systémoch Mesta. Prostredníctvom implementácie odporúčaných opatrení a postupov sa bude Mesto Banská Bystrica ako prevádzkovateľ základnej služby efektívnejšie brániť proti identifikovaným bezpečnostným hrozbám;
- Realizáciou tejto aktivity sa okrem naplnenia minimálnych požiadaviek poskytovateľa NFP odstráni aktuálny stav v oblasti governance informačnej a kybernetickej bezpečnosti, kedy Mesto okrem zriadeného Bezpečnostného výboru nedisponuje žiadnou vypracovanou bezpečnostnou dokumentáciou a teda riadenie IB a KB sa zmení z neformálne riadeného na formálne a procesne riadené s jasne popísanými úrovňami zodpovedností a právomocí;

3. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta

- Nasadením platformy pre správu prístupov sa napomôže vyriešiť problém neoprávneného prístupu k sieti pomocou autentifikácie a autorizácie používateľov a zariadení a odstráni sa súčasný stav, ktorý sa vyznačuje nízkou efektivitou a nízkou flexibilitou pri správe identít a prístupových práv v sieti;
- Rozšíria sa možnosti kategorizácie používateľov a zariadení (profilácia), čím Mesto Banská Bystrica nadobudne väčšiu flexibilitu selekcie prideľovania prístupov vybraným typom používateľov a/alebo zariadení;
- Zvýšenie úrovne zabezpečenia pred bezpečnostnými hrozbami prostredníctvom zvýšenia počtu a dostupnosti prístupových politík a politík kontroly, čím sa zníži riziko neoprávneného prístupu do siete Mesta;
- Odstránenie súčasne nízkeho stavu auditovateľnosti prihlasovania sa používateľov a/alebo zariadení do siete Mesta;
- Zjednodušenie riadenie prístupu pre rôzne typy používateľov a zariadení za súčasného odbúravania agendy personálu zodpovedajúceho za prevádzku IKT, IB a KB;
- Výmenou switchov, ktoré sú end-of-sale a end-of-support za nové, ktoré majú podporu protokolu IEEE 802.1X sa zníži riziko výpadkov v sieti, zabezpečí kontinuita podpory a záplat na HW infraštruktúre ako aj súlad so všeobecne platnými praktickými pravidlami potreby nahradiť end-of-support produkty za tie, ktoré sú podporované.

4. Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky

- Vykonaním segmentácie siete Mesta Banská Bystrica sa odstráni súčasný stav, kedy sa v prípade úspešného útoku tento má možnosť šíriť po celej sieti. Realizáciou segmentácie sa dosiahne stav, kedy sa zúži možnosť šírenia útokov a hrozieb na úroveň vytvorených segmentov;
- Segmentácia prispeje k odstráneniu stavu, kedy autorizovaný a autentifikovaný užívateľ má prístup do celej siete a nie iba do časti, do ktorej má mať prístup vzhľadom na jeho príslušnosť do skupiny používateľov / zariadení;
- Vykonaním segmentácie siete sa očakáva optimalizácia výkonu siete a to oddelením prevádzky prioritných aktív od menej prioritných;
- Zjednodušenie a zrýchlenie diagnostiky siete po vykonaní segmentácie vzhľadom na skutočnosť, že po vykonaní segmentácie bude možné jednoduchšie lokalizovať a diagnostikovať prípadné problémy so sieťovou dostupnosťou alebo výkonom na úrovni konkrétneho segmentu siete;

5. Dodávka aktívnych prvkov CORE časti siete

- Nákupom nových aktívnych prvkov CORE časti siete Mesta sa zníži riziko výpadkov v sieti, zabezpečí kontinuita podpory a záplat na CORE HW sieťovej infraštruktúre, nakoľko v súčasnosti Mesto Banská Bystrica na úrovni CORE časti siete disponuje zariadeniami, ktoré sú end-of-sale a end-of-support;
- Nákupom nových aktívnych prvkov sa doplní CORE časť siete, čím sa podporí zabezpečenie kontinuity požadovanej úrovne IT aktív, ako aj primerané doby odozvy informačných aktív v sieti Mesta;
- Jedným z hlavných problémov, ktorý rieši táto aktivita je, že nové zariadenia pre CORE časť siete umožnia vykonať realizáciu aktivity č.3 ako aj č.4 keďže nové zariadenia budú podporovať protokol IEEE 802.1X pre účely nasadenia systému riadenia a správy prístupov koncových zariadení a to aj v kontexte uvažovanej segmentácie siete;
- Nákupom nových aktívnych prvkov CORE časti siete sa súčasne očakáva zvýšenie úrovne spoľahlivosti siete, keďže Mesto Banská Bystrica očakáva, že nové, výrobcom podporované a moderné aktívne prvky disponujú vyššou mierou odolnosti voči výpadkom a poruchám v porovnaní s jestvujúcimi zariadeniami.

6. Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete

- Implementáciou systému dvojfaktorového overovania Mesto Banská Bystrica očakáva zvýšenie úrovne zabezpečenia prístupu používateľov do siete prostredníctvom pridania ďalšieho faktora overenia voči súčasnému stavu, ktorý od užívateľov vyžaduje pri prihlásení sa do siete iba kombináciu mena a hesla, čo môže napr. pri phisingovej kampani útočník prelomiť a získať prístup k aktívam Mesta bez potreby vykonania ďalšieho kroku pri prístupe do siete;
- Implementáciou riešenia sa očakáva súčasne dodržiavanie bezpečnostných predpisov a noriem resp. zistení, ktoré boli identifikované počas vykonávaných auditov KB. Zodpovedný certifikovaný audítor opakovane v zisteniach uviedol nevyhnutnosť zabezpečenia prístupu do siete Mesta prostredníctvom zavedenia ďalšieho faktora overovania. Na základe uvedeného Mesto túto aktivitu považuje za absolútne kľúčovú, keďže dlhodobým zámerom mesta je držať vysokú úroveň IB a KB aj v kontexte identifikovaných zistení.
- Zavedením dvojfaktorového overovania sa zároveň zvýši úroveň zabezpečenia vzdialeného prístupu do siete Mesta z externého prostredia, ktorého úroveň zabezpečenia nemá Mesto pod kontrolou.

7. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

- Nasadením riešenia centrálneho bezpečnostného manažmentu pre koncové stanice Mesto Banská Bystrica zvýši úroveň zabezpečenia koncových staníc ako aj zvýši efektivitu riadenia prevádzky koncových staníc, nakoľko realizáciou tejto aktivity očakáva nadobudnutie možnosti centralizovanej správy zariadení ako aj centrálneho sledovania správania na koncových staniciach;

- Riešenie zvýši viditeľnosť personálu zodpovedného za riadenie prevádzky a správy aktív ako aj IB a KB, nakoľko riešenie prinesie zvýšenú úroveň a granularitu monitoringu koncových staníc ako aj získanie informácií o klientoch na koncových staniciach v reálnom čase;
- Súčasne bude prevádzkový personál disponovať nástrojom, ktorý generuje notifikácie v prípade výskytu neočakávaných situácií, čo rovnako zvýši možnosť koncentrovať sa udalosti s vyššou prioritou;

Podpora business procesov

Realizáciou aktivít projektu nedôjde k zmenám na strane súčasne nastavených business procesov. Jednotlivé organizačné útvary mesta, ako aj organizácie v zriaďovateľskej pôsobnosti mesta, príspevkové organizácie, ktoré realizujú business procesy na dennej báze nebudú v oblasti výkonu ich nastavených business procesov priamo ovplyvnené. Realizácia aktivít projektu bude mať predovšetkým podporný charakter, keďže plošne na úrovni siete Mesta Banská Bystrica budú zabezpečené informačné aktíva, ktoré sú využívané v jednotlivých vykonávaných business procesoch vykonávaných v rámci ISVS, ktoré Mesto Banská Bystrica súčasne uvádza v META IS:

Názov	Kód Meta IS	Stav
Mobilná aplikácia RON	Isvs_11928	V prevádzke
RON Jedáleň aplikácia	Isvs_11927	V prevádzke
RON jedálenský systém	Isvs_11926	V prevádzke
RON dochádzkový systém	Isvs_11925	V prevádzke
Pohoda – ekonomický softvér	Isvs_11924	V prevádzke
SPIN – pult centrálnej ochrany MsP	Isvs_11917	V prevádzke
SHERIFF – IS mestskej polície	Isvs_11916	V prevádzke
MS Office365	Isvs_11915	V prevádzke
IS HER pre rokovanie MsR a MsZ	Isvs_11914	V prevádzke
GScan – scanovací modul	Isvs_11913	V prevádzke
GISPlan – geograficky IS	Isvs_11912	V prevádzke
eZákazky – softvér	Isvs_11911	V prevádzke
Systém pre verejné obstarávanie – eBiz	Isvs_11910	V prevádzke
aScOrbit	Isvs_11909	V prevádzke
aSc Agenda	Isvs_11908	V prevádzke
Webové sídlo Mesta Banská Bystrica	Isvs_11907	V prevádzke
Registratúrny systém CG DISS	Isvs_11906	V prevádzke
Intranetový Portál mesta	Isvs_11904	V prevádzke
Portálový modul CG Datamesta	Isvs_11903	V prevádzke
Portálový modul CG eGOV	Isvs_11902	V prevádzke
Modul integrácie na externé IS .COMM ISS	Isvs_11901	V prevádzke
Personalistika a mzdy CG ISS	Isvs_11900	V prevádzke
Ekonomika CG ISS	Isvs_11899	V prevádzke
BASE CG ISS	Isvs_11898	V prevádzke
Informačný systém mesta CG ISS	Isvs_11897	V prevádzke
Informačný systém Digitálna technická mapa a digitálny územný plán	Isvs_11468	V pláne vybudovať
Podpora asistovaného života seniorov	Isvs_11066	V pláne vybudovať
Manažment s podporou IoT	Isvs_11065	V pláne vybudovať
Platforma SMART CITY	Isvs_10386	V prevádzke

Na základe uvedeného možno sumarizovať nasledovné hlavné business procesy, ktoré budú podporené zvýšenou úrovňou zabezpečenia:

- Správa financií a rozpočtu;
- Správa miestnych poplatkov a daní (registrovanie a výber poplatkov za psa);
- Riadenie a kontrola dochádzky zamestnancov;
- Výkon dohľadu nad bezpečnosťou verejných priestranstiev;
- Riadenie procesu obstarávania tovarov, služieb a stavebných zákaziek;
- Personálna a mzdová agenda;
- Správa mestskej infraštruktúry a stavebná agenda (zriaďovanie vecného bremena na majetok Mesta / vydávanie rozhodnutí o zvláštnom užívaní miestnej komunikácie /);
- Matrika – evidencia udalostí, správa evidencie a údajov o identite a občianstve, vybavovanie žiadostí;
- Sociálna agenda a školstvo;
- Agenda životného prostredia (vydávanie rozhodnutí o výrube dreviny)
- Agenda dopravy (vyhradzovanie parkovacieho miesta za poplatok / vydávanie parkovacej karty / určovanie trvalého alebo prenosného dopravného značenia);

Podrobný zoznam business procesov realizovaných prostredníctvom identifikovaných ISVS je možné stotožniť s poskytovanými koncovými službami Mesta, ktorých podrobný zoznam je uvedený tu: https://metais.vicepremier.gov.sk/detail/PO/63fd37ae-5ee8-413d-9141-c259f190d310/cimaster?tab=relationsForm.

Realizácia projektu ako aj jeho očakávané výsledky a výstupy priamo nerieši životné situácie, ich organizáciu a charakter a ani nevytvára zmeny v jestvujúcich životných situáciách prostredníctvom ktorých interaguje Mesto Banská Bystrica s obyvateľmi, návštevníkmi alebo podnikateľskou sférou. Zvýšenie úrovne kybernetickej a informačnej bezpečnosti nevyvolá zmenu charakteru poskytovaných služieb horeuvedeným skupinám, ale prispeje k zvýšeniu úrovne zabezpečenia informačných aktív, ktoré sú pri výkone agendy v oblasti životných situácií využívané. Možno konštatovať, že projekt zabezpečí okrem vyššej úrovne bezpečnosti aj vyššiu úroveň odolnosti služieb a teda aj ich celkovej dostupnosti pre dotknutých stakeholderov. Horeuvedené ISVS tak zvýšia stabilitu poskytovaných služieb mesta napr. pri nasledovných životných situáciách:

- Narodenie dieťaťa;
- Úmrtie;
- Zmena osobných údajov;
- Zmena trvalého / prechodného pobytu...

Motiváciou na dosiahnutie budúceho požadovaného stavu bolo predovšetkým nasledovné:

- Ambícia Mesta Banská Bystrica reflektovať na aktuálne hrozby a výzvy v oblasti IB a KB;
- Zrealizovaný a vykonávaný audit KB;
- Ochrana reputácie Mesta Banská Bystrica ako prevádzkovateľa základnej služby;
- Ochrana dôvernosti a integrity údajov spracúvaných v informačných aktívach Mesta;
- Dodržiavanie súladu s aktuálne platnou legislatívou;
- Zabezpečenie kontinuity prevádzky informačných aktív;
- Zlepšenie internej efektivity a efektívnosti pri správe a dohľade nad informačnými aktívami Mesta.

3.3 Zainteresované strany/Stakeholderi

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Mesto Banská Bystrica	Mesto BB	Vlastník informačných aktív a monitorovaný subjekt, prevádzkovateľ základnej služby	Viď tabuľka - časť 3.2 tohto dokumentu
2.	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	MIRRI	Gestor eGovernmentu, riadiaci orgán	Nerelevantné
3.	Občan/podnikateľ/návštevník mesta	FO/PO	užívateľ	Nerelevantné
4.	Orgány verejnej moci a ich podsektory	OVM	Zdieľanie dát medzi ISVS OVM a ISVS Mesta BB	

3.4 Ciele projektu

ID	Názov cieľa	Názov strategického cieľa	Spôsob realizácie strategického cieľa
1.	Zaistenie kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB.	Zabezpečiť primeranými technickými, organizačnými a personálnymi bezpečnostnými opatreniami ochranu dôvernosť, integrity a dostupnosti informačných aktív (Stratégia KB, MIRRI)	1. Vykonanie opakovaného auditu informačnej a kybernetickej bezpečnosti v súlade s § 9 Zákona o KB; 2. Vypracovanie relevantnej bezpečnostnej dokumentácie; 3. Implementácia systému pre inventarizáciu aktív a harmonizáciu procesov v oblasti IB a KB; 4. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica; 5. Vykonanie segmentácie siete Mesta Banská Bystrica s ohľadom na súčasné prevádzkové požiadavky; 6. Výmena aktívnych prvkov CORE časti siete;

			7. Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete; 8. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice;
2.	Zaistenie kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB.	Zvyšovať povedomie o informačnej a kybernetickej bezpečnosti všetkých zamestnancov a vedenia organizácie	Realizácia školenia dotknutého personálu na implementované technológie.

3.5 Merateľné ukazovatele (KPI)

ID	ID/Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merateľné hodnoty (aktuálne)	TO BE Merateľné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
1.	PO095/PSKPS0I12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne, napríklad v kontexte opatrení smerujúcich k elektronickej verejnej správy.	Verejné inštitúcie	0	1	Preverí sa, skutočný počet podporených subjektov verejnej správy zapísaných v štatistickom registri organizácií vedenom Štatistickým úradom SR, ktoré sú zaradené v sektore verejnej správy, v rámci ktorých došlo k modernizácii služieb, produktov, procesov a zvýšeniu vedomostnej úrovne v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy	Aktivity projektu realizované na úrovni Mesta Banská Bystrica.
2.	PR017/PSKPRCR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Počet nových a vylepšených verejných digitálnych služieb, produktov a procesov	Používatelia / rok	0	250	Preverí sa, počet zamestnancov, ktorí sú používateľmi nových a vylepšených digitálnych služieb	„TO-BE" bude zodpovedať počtu zamestnancov, ktorí vykonávajú svoje činnosti na zabezpečených informačných aktívach, ktorých zabezpečenie je predmetom projektu.
3.	PR017 / PSKPRCR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Nová verejná digitálna služba, produkt alebo proces	Používatelia / rok	0	250	Preverí sa počet zamestnancov, ktorí sú používateľmi novej verejnej digitálnej služby, produktu alebo procesu	Nové produkty ako výsledok projektu, preverí sa preukázaním dokumentácie a/alebo prostredníctvom preberacích protokolov a/alebo dátových

								listov k dodaným produktom.

3.6 Špecifikácia potrieb koncového používateľa

n/a

3.7 Riziká a závislosti

Vo procese spracovania tohto dokumentu Mesto Banská Bystrica identifikovalo nasledovné riziká:

A. Omeškanie alebo zrušenie procesu verejného obstarávania;
B. Personálne kapacity na strane Mesta Banská Bystrica;
C. Kapacity a odbornosť na strane dodávateľa/dodávateľov;
D. Havária niektorého z dotknutých ISVS alebo časti siete nezapríčinená Mestom a/alebo dodávateľom/dodávateľmi;
E. Legislatívne zmeny, zmeny v riadiacej dokumentácii.

Podrobnejšie informácie o rizikách a závislostiach sú uvedené v samostatnom dokumente „Zoznam rizík a závislosti“, ktorý bude počas ďalších etáp projektu aktualizovaný na pravidelnej báze. Súčasne budú riziká vyhodnocované na dvoch úrovniach:

- „high-level“ – riziká s dopadom na realizáciu plánu projektu a progresu projektových aktivít;
- „low-level“ – riziká s menším dopadom a dopadom predovšetkým na úrovni dodávky predmetu projektu „delivery level“.

Procesné riadenie rizík bude podrobne popísané v rámci Projektového iniciálneho dokumentu („PID“), v prípade, že bude projekt oficiálne spustený. V rámci PID budú definované spôsoby a stratégie riadenia rizík ako aj ich komunikácie v priebehu celého projektu.

3.8 Stanovenie alternatív v biznisovej vrstve architektúry

Na riešenie problémovej situácie boli identifikované možné alternatívne/variantné riešenia:

	Budúci možný stav			
Súčasný stav	**Možný variant**	**Biznis vrstva**	**Aplikačná vrstva**	**Technologická vrstva**
Nedostatočná úroveň zabezpečenia IB a KB v Meste Banská Bystrica	Nulový variant	Pokračovať v súčasnom stave bez nutnosti realizácie projektu	Využiť súčasnú, pre realizáciu všetkých aktivít projektu nepostačujúcu, úroveň aplikačnej vrstvy pri zachovaní stavu „AS-IS“	Realizovať len nákup HW s obmedzenom počte sieťových prvkov bez výmeny aktívnych prvkov bez podpory IEEE 802.1X
	Optimálny variant (celý rozsah projektu)	**Realizovať projekt v plnom rozsahu**	**Doplniť súčasnú aplikačnú vrstvu o nové prvky potrebné pre zvýšenie úrovne IB a KB a vykonať implementáciu a konfiguráciu služieb tak, aby bol využitý maximálny potenciál a funkcionalita súčasných ako aj navrhovaných riešení**	**Implementovať všetky funkcionality, kompletný rozsah nástrojov a vytvoriť bezpečný kybernetický priestor**
	Limitovaný variant	Pre realizáciu projektu využiť len realizáciu vybraných aktivít dvojfaktorové overovanie, realizácia opakovaného auditu KB a vypracovanie relevantnej bezpečnostnej dokumentácie	Nasadiť iba moduly s obmedzenou funkcionalitou, resp. vybrať iba tie, ktoré sú z pohľadu vykonaného auditu KB s najvyššou prioritou (riešenie 2 faktorovej autentifikácie)	Realizovať len nákup HW komponentov potrebných pre implementáciu dvojfaktorového overovania, bez výmeny HW v CORE časti siete a výmeny zariadení s podporou IEEE 802.1X

Pri realizácii projektu je možné na základe vykonanej analýzy postupovať troma nasledovnými alternatívami:

A. Nulový variant: Zachovať súčasný stav, a jednotlivé navrhované aktivity projektu realizovať čiastkovo bez vzájomného koordinovaného postupu. Tento variant je síce najlacnejší z pohľadu úspor za nezrealizované aktivity, avšak navrhované aktivity projektu reflektujú legislatívne požiadavky a povinnosti Mesta Banská Bystrica na zabezpečenie svojich informačných aktív. Je dôvodné očakávať, že nerealizovanie projektu (akceptácia nulového variantu) by viedla k dodatočným nákladom presahujúcim nakumulované úspory – neodporúča sa.

B. Optimálny variant: Realizácia aktivít projektu v celom ich rozsahu so zohľadnením východiskového stavu. Aktivity projektu boli volené na základe skutočných potrieb Mesta Banská Bystrica a dôrazom na ich vzájomné technické ako i procesné prepojenie, preto je účelné ich realizovať v rámci jedného projektu vo vzájomne súvisiacich pracovných balíkoch. Realizácia projektu v optimálnom variante zároveň vyrieši všetky súčasne identifikované zásadné nedostatky v oblasti IB a KB, ktoré sú Mestu známe.

C. Obmedzený variant: Tento variant počíta s realizáciou aktivít projektu s najvyššou prioritou a to i napriek tomu, že všetky navrhované aktivity možno považovať za prioritné. V tomto variante sa počíta s nasadením riešenia dvojfaktorovej autentifikácie ako niekoľkokrát opakovaného zistenia auditov KB, súčasne navrhuje realizáciu resp. ukončenie opakovaného auditu, ktorý bol zahájený po 20.02.2024 ako aj s vypracovaním relevantnej bezpečnostnej dokumentácie na úrovni organizácie, keďže Mesto ňou v súčasnosti nedisponuje. V tomto variante sa

D. nepočíta s nákupom HW komponentov s podporou IEEE 802.1X a súvisiacimi aktivitami ako segmentácia siete. V tomto prípade, by síce došlo k odstráneniu zásadných nedostatkov identifikovaných auditmi KB, avšak úroveň IB a KB by nebola zabezpečená na takej úrovni ako je účelné ju riešiť v optimálnom variante a to aj z dôvodu, že jednotlivé aktivity sú navzájom v prieniku, čo pri súčasnej implementácii povedie k úspore min. v oblasti riadenia projektu. Zároveň je možné očakávať, že nerealizované aktivity v tomto variante bude potrebné tak či onak realizovať, pričom nemožno očakávať, že ich realizácia v budúcnosti bude možná za rovnakých alebo výhodnejších podmienok.

Odporúčanie: Navrhuje sa realizovať Optimálny variant.

3.9 Multikriteriálna analýza

Kritériá pre MCA

	KRITÉRIUM	ZDÔVODNENIE KRITÉRIA	Občan / podnikateľ	Zamestnanec	Mesto BB	Podriadené organizácie
Stanovené alternatívy	Kritérium A (KO) - komplexná identifikácia aktuálnych hrozieb	Realizácia projektu zabezpečí komplexnú analýzu a následnú identifikáciu hrozieb, ktoré prispeje k efektívnemu nasadzovaniu preventívnych opatrení		X	X	X
	Kritérium B (KO) - súlad s legislatívnymi požiadavkami na úrovni governance a procesov v oblasti IB a KB	Zabezpečí sa vypracovanie kompletnej dokumentácie v súlade s aktuálne platnou legislatívou v oblasti IB a KB ako aj vypracovanie interných riadiacich aktov pre oblasť IB a KB		X	X	X
	Kritérium C (KO) - zabezpečenie vyššej úrovne prístupu do siete	Prispeje k posilneniu bezpečnosti pri prístupe používateľov do siete o pridanie druhého faktora		X	X	X
	Kritérium D -lepšie a efektívnejšie využite nových technológií	Nové funkcionality výrazne zvyšujú schopnosť ochrany pred kybernetickými bezpečnostnými incidentami		X	X	X
	Kritérium E Vytvorenie pokročilého systému autentifikácie a autorizácie v sieti mesta na úrovni skupín používateľov	Riadenie prístupov do siete Mesta Banská Bystrica vrátane vykonania segmentácie, tvorby skupín zariadení a používateľov (profily), zabezpečenie prístupov zariadení a používateľov na úrovni portu na aktívnom prvku	X	X	X	X

	Kritérium F Centralizovaný dohľad a správa nad informačnými aktívami	Zabezpečenie nástrojov na ochranu, monitoring a centrálny dohľad nad aktívami Mesta Banská Bystrica		X	X	X

Vyhodnotenie MCA

Zoznam kritérií	Alternatíva1	Spôsob dosiahnutia	Alternatíva 2	Spôsob dosiahnutia	Alternatíva 3	Spôsob dosiahnutia
Kritérium A	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 zabezpečí komplexnú analýzu a identifikáciu hrozieb	áno	Implementácia alternatívy č. 3 zabezpečí komplexnú analýzu a identifikáciu hrozieb
Kritérium B	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 zabezpečí vypracovanie kompletnej dokumentácie v súlade s aktuálne platnou legislatívou v oblasti IB a KB ako aj vypracovanie interných riadiacich aktov pre oblasť IB a KB	áno	Implementácia alternatívy č. 3 zabezpečí vypracovanie kompletnej dokumentácie v súlade s aktuálne platnou legislatívou v oblasti IB a KB ako aj vypracovanie interných riadiacich aktov pre oblasť IB a KB
Kritérium C	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 Prispeje k posilneniu bezpečnosti pri prístupe používateľov do siete o pridanie druhého faktora overenia	áno	Implementácia alternatívy č. 3 Prispeje k posilneniu bezpečnosti pri prístupe používateľov do siete o pridanie druhého faktora overenia
Kritérium D	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 pomocou implementácie nových funkcionalít navrhovaných projektom výrazne zvýši schopnosť ochrany pred kybernetickými bezpečnostnými incidentami	Čiastočne áno	Implementácia alternatívy č. 3 pomocou nových funkcionalít v obmedzenom rozsahu zvýši čiastočne schopnosť ochrany pred kybernetickými bezpečnostnými incidentmi.
Kritérium E	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 Zabezpečí riadenie prístupov do siete Mesta Banská Bystrica vrátane vykonania segmentácie, tvorby skupín zariadení a používateľov (profily), zabezpečí prístupy zariadení a používateľov na úrovni portu na aktívnom prvku	nie	Zachovanie súčasného stavu
Kritérium F	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 Zabezpečí nástroje na ochranu, monitoring a centrálny dohľad nad aktívami Mesta Banská Bystrica	nie	Zachovanie súčasného stavu

3.10 Stanovenie alternatív v aplikačnej vrstve architektúry

Alternatívy na úrovni aplikačnej architektúry reflektujú alternatívy vypracované na základe „nadradenej“ architektonickej biznis vrstvy, pričom vďaka uplatneniu nasledujúcich princípov aplikačná vrstva architektúry dopĺňa informácie k alternatívam stanoveným pomocou biznis architektúry.

V nadväznosti na stanovenie alternatív business vrstvy, za najvýhodnejšiu sa v kontexte legislatívnych požiadaviek, východiskového stavu, prevádzkových a administratívnych nákladov považuje Alternatíva č.2.

3.11 Stanovenie alternatív v technologickej vrstve architektúry

Výber alternatívy na úrovni technologickej vrstvy reflektuje a kopíruje výber Alternatívy č.2 na základe MCA. Riešenie Alternatívy č.2 (ako aj ostatné uvažované alternatívy) sa plánuje nasadiť na infraštruktúre Mesta Banská Bystrica. Všetky HW komponenty, ktoré sú predmetom projektu budú fyzicky dodané, umiestnené a inštalované v prostredí Mesta.

S využitím vládneho cloudu sa aj s ohľadom na charakter projektu nepočíta. Z ohľadom na uvedené nebolo nutné vykonať analýzu posúdenia finančnej udržateľnosti a výhodnosti riešenia vládneho cloudu vo vzťahu k iným alternatívam.

Celkové výdavky projektu v štandardizovanom členení, t.j. s uvedením CAPEX a OPEX sú uvedené nižšie v tomto dokumente v časti „Rozpočet projektu“.

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

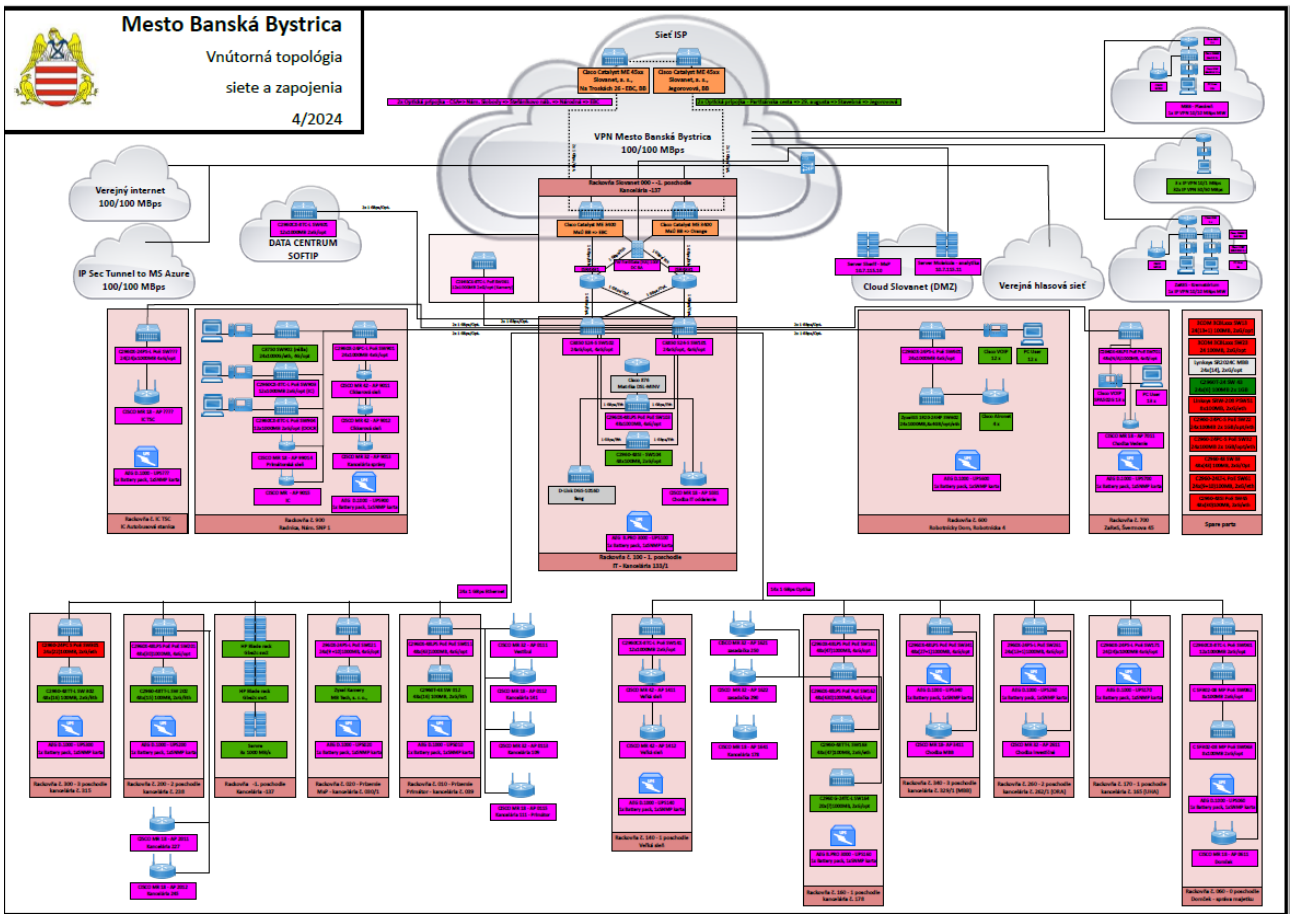
Požadovaným výstupom projektu je funkčné, dlhodobo udržateľné a ucelené riešenie pre zvýšenie úrovne IB a KB, ktoré pozostáva z viacero navzájom súvisiacich produktov projektu. Podrobnejší popis výstupov projektu sumarizuje nasledovná tabuľka:

ID	Výstup projektu – názov	Popis / poznámka
1.	Vykonaný opakovaný audit projektu	Výstupom opakovaného auditu bude správa audítora KB v súlade so Zákonom o KB
2.	Vypracovaná bezpečnostná dokumentácia	Výstupom bude vypracovaná bezpečnostná dokumentácia v súlade so Zákonom o KB a Vyhláškou o KB v rozsahu uvedenom v časti 3 tohto dokumentu
3.	Nasadené riešenie správy prístupov koncových zariadení do siete Mesta	Výstupom bude nasadené riešenie správy prístupov koncových zariadení do siete Mesta založené na protokole IEEE 802.1X vrátane dodávky 7 ks switchov, ktoré podporujú protokol 802.1X.
4.	Vykonaná segmentácia siete	Výstupom projektu bude vykonaná segmentácia siete v súlade s vykonanou analýzou, ktorú zabezpečia externé kapacity dodávateľa na základe získaných informácií počas etapy analýza a dizajn. Výstupom bude súčasne konfiguračná dokumentácia.
5.	Dodané aktívne prvky CORE časti siete	Výstupom bude dodaných celkovo 9 ks aktívnych sieťových prvkov s podporou IEEE 802.1X.
6.	Nasadený systém dvojfaktorovej autentifikácie	Výstupom bude nasadený systém dvojfaktorovej autentifikácie s klientami a tokenmi pre 700 používateľov (50 ks HW token + 650 ks SW token).
7.	Nasadené riešenie centrálneho bezpečnostného manažmentu	Výstupom bude nasadený systém uceleného riešenia centrálnej správy koncových staníc pre 700 ks koncových staníc.
8.	Projektové výstupy – dokumentácia	Výstupom bude súbor dokumentácie vypracovanej v zmysle Vyhlášky 401/2023 Z.z. o riadení projektov v rozsahu a kontexte zodpovedajúcemu rozsahu projektu. Ucelený zoznam požadovaných výstupov (produktov projektu vrátane manažérskych produktov) bude uvedený v Projektovom iniciálnom dokumente („PID“) v následnej fáze projektu.

Výstupmi projektu nebudú žiadne koncové služby ani biznis objekty, ktoré možno klasifikovať ako výstupy zo systému (napr. podania, formuláre, rozhodnutia, reporty, dáta, aplikačné rozhrania...). Vlastníkom výstupov ako aj procesu bude zástupca Mesta, ktorý bude súčasne zastávať pozíciu kľúčového používateľa.

5. NÁHĽAD ARCHITEKTÚRY

V náhľade nižšie uvádzame pohľad na komplexnú sieťovú architektúru Mesta. Realizáciou aktivít projektu nedôjde k zmene topológie siete, ani zmene na úrovni dátovej architektúry.



Zmeny na úrovni business architektúry budú minimálne a to vo väzbe na nutnosť zadávania druhého faktora v riešení dvojfaktorového overovania, kedy používateľ okrem mena a hesla bude nútený zadať druhý prístupový kód generovaný HW alebo SW tokenom.

Platforma pre správu prístupov:

Centralizovaný manažment a správa	• centrálna konfigurácia a správa profilov, prístupov, hostí, autentifikácia a autorizácia služieb v jednoduchom web grafickom rozhraní;
Riadenie politík	• možnosť nastavovania politík prístupu na základe definovaných pravidiel; • možnosť tvorby modelov prístupu na základe definície rôznych atribútov ako sú identita používateľa / zariadenia, autentifikačné protokoly, identita koncového zariadenia; • možnosť dynamickej definície a nastavovania atribútov; • možnosť integrácie na Microsoft Active Directory, LDAP, RADIUS, RSA OTP.
Riadenie prístupov	• na základe Access Control Lists (dACLs), priradeniu k VLAN, URL presmerovania, ACLs, SGACLs.
Riadenie šifrovania	• možnosť editácie zoznamu používaného šifrovania, ktoré môže byť zakázané pre účely vynútenia bezpečnostných politík organizácie; • možnosť vynútenia využívania povoleného typu šifrovania pri autentifikácii.
AI/ML profilovanie a viacfaktorová klasifikácia	• možnosť rýchlej identifikácie neznámych koncových zariadení prostredníctvom cloudového ML engine; • možnosť revízie zariadení prostredníctvom profilových politík použitím ML engine; • možnosť tvorby prístupových skupín koncových zariadení prostredníctvom profilov a pravidiel vytvorených správcom siete;
Prístup do siete	• možnosť rýchleho nasadenia zabezpečeného prístupu k sieti prostredníctvom autentifikácie a autorizácie na základe údajov získaných z prihlasovacích údajov na rôznych aplikačných úrovniach.
Riadenie politiky prístupových skupín	• podpora jednoduchej segmentácie prostredníctvom bezpečnostných tagov; • funkcionalita správy segmentácie a zjednodušenej správy prepínačov, smerovačov, bezdrôtových zariadení a pravidiel pre firewally.

Pridávanie zariadení do siete	• podpora automatizovaného poskytovania a registrácie certifikátu pre štandardné PC a mobilné zariadenia;
AAA služby	• podpora RADIUS protokolu pre autentifikáciu, autorizáciu a accouting (AAA); • podpora protokolov PAP, MS-CHAP, EAP-MD5, PEAP, EAP-Flexible, TEAP; • podpora autentifikácie cez tunel prostredníctvom protokolu FAST, TLS, TTLS.
Správa prístupov zariadení	• podpora protokolu TACACS+; • podpora prístupu používateľa na základe lokality, skupiny, prihlasovacích údajov;
Profilovanie zariadení	• podpora preddefinovaných šablón koncových zariadení ako sú IP telefóny, kamery, smartfóny, tablety, tlačiarne; • možnosť tvorby vlastných šablón zariadení pre potreby automatického zistenia, klasifikácie a priradenia identít pri pripájaní sa do siete; • možnosť priraďovania autorizačných politík špecifických pre koncový bod na základe identifikovaného typu zariadenia; • možnosť zberu údajov o atribútoch koncového bodu pomocou pasívneho monitorovania siete a telemetrie.
Hodnotenie zariadení pripojených do siete	• podpora vyhodnocovania koncových zariadení pripojených v sieti; • podpora vytvárania politík na kontrolu najnovších záplat OS, kontrolu aktuálnych verzií antivírusových a antispyware balíkov, kontrolu pravidiel šifrovania disku, prítomnosti aplikácií a pod. • podpora plnej viditeľnosti HW zariadení v sieti;
Podpora Active Directory	• podpora autentifikácie a autorizácie použitím multistromových Microsoft AD domén; • podpora grupovania viacerých nespojených domén do logických skupín; • možnosť flexibilného prepisovania pravidiel identít; • podpora Microsoft AD 2003, 2008, 2008R2, 2012, 2012R2, 2016 a 2019
Monitoring a riešenie problémov	• integrovaná konzola s webovým rozhraním pre účely monitorovania, generovania správ a riešenia problémov; • podporuje funkcionalitu záznamu všetkých aktivít a metrík v reálnom čase na úrovni všetkých používateľov a koncových bodov, ktoré sú pripojené v sieti.
Spôsob nasadenia	• možnosť nasadenia v prostredí verejného obstarávateľa v režime vysokej dostupnosti „HA“. Prostredie virtualizácie a výpočtové zdroje poskytne verejný obstarávateľ.

Switch TYP 1 (7ks)	
Porty	• 24 portov 10/100/1000 Ethernet PoE+
Uplink rozhrania	• 4 x 1G SPF uplink
CPU	• ARM v 7 800 MHz
PoE+ power budget	• 195 W
DRAM	• 512 MB
Flash pamäť	• 256 MB
Šírka pásma – forwarding	• 28 Gbps
Šírka pásma – switching	• 56 Gbps
Rýchlosť preposielania (64 byte L3 paketov)	• 41,67 Mpps
Unicast MAC adresy	• 16000
IPv4 unicast direct routes	• 542
IPv4 unicast indirect routes	• 256
IPv6 unicast direct routes	• 414
IPv6 inicast indirect routes	• 128
IPv4 multicast routes a IGMP skupiny	• 1024
IPv6 multicast skupiny	• 1024
Maximálny počet aktívnych VLAN	• 256
MTU-L3 paket	• 9198 bajtov
Jumbo ethernet rámce	• 10 240 bajtov

Dodávka aktívnych prvkov CORE časti siete

- bez zmeny sieťovej a bezpečnostnej architektúry, jedná sa o technologický upgrade.

Firewall CORE časť - TYP 1 (2 ks)	
GE RJ-45 porty	• 16 ks
GE RJ-45 porty – manažment HA	• 1 ks
GE SFP slot	• 8 ks
10 GE SFP+	• 2 ks
USB port	• 1 ks
Konzolový port	• 1 ks
Vnútorné úložisko	• 480 GB SSD
IPS priepustnosť	• 5 Gbps
NGFW priepustnosť	• 3.5 Gbps
Ochrana pred hrozbami – priepustnosť	• 3 Gbps
UPv4 priepustnosť firewallu (1518 / 512 / 64 bajtov, UDP)	• 27 / 27 / 11 Gbps
Priepustnosť firewallu (paket / sekunda)	• 16.5 Mpps
Počet súčasných spojení (TCP)	• 3 000 000
Počet nových spojení TCP / sekunda	• 280 000
Počet politík FW	• 10 000
Priepustnosť IPsec VPN (256 bajtov)	• 13 Gbps
Počet GW to GW IPsec VPN tunelov	• 2 000
Počet klient – klient IPsec VPN tunelov	• 16 000
Priepustnosť SSL-VPN	• 2 Gbps
Počet súčasných SSL-VPN používateľov	• 500
Priepustnosť SSL inšpekcie	• 4 000 Gbps
SSL inšpekcia CPS	• 3 500
Počet súčasných spojení SSL inšpekcia	• 300 000
Priepustnosť kontroly aplikácií	• 13 Gbps
CAPWAP priepustnosť	• 20 Gbps
Počet virtuálnych domén	• 10
HA konfigurácia	• active-active, active-passive, clustering

Switch CORE časť - TYP 1 (2 ks)	
10/100/1000 porty	• 24x 1G SFP
Pamäť DRAM	• 8 GB
Pamäť flash	• 16 GB
Počet VLAN IDs	• 4094
Uplink konfigurácia	• Modulárna
Kapacita prepínania	• 208 Gbps
Stakovacia šírka pásma	• 688 Gbps
Rýchlosť preposielania	• 154,76 Mpps
Celový počet MAC adries	• 32 000
IPv4 direct routes	• 24 000
IPv4 indirect routes	• 8 000
IPv6 routes	• 16 000
Rozsah multicast routing	• 8 000
Rozsah QoS záznamov	• 5 120
Rozsah ACL záznamov	• 5 120
Jumbo ethernet rámce	• 9198 bajtov
Príslušenstvo – stohovací kábel 1	• 2x stohovací kábel; • Kompatibilný so Switch CORE TYP 1; • Dĺžka 0,5 m.
Príslušenstvo – stohovací kábel 2	• 2ks stohovací kábel; • Kompatibilný so Switch CORE TYP 1; • Možnosť sériového napájania zariadení; • Dĺžka 1,5 m.

Príslušenstvo – sieťový modul	• 10 GE SFP+; • Rýchlosť 1G/10Gb/s; • Chladenie pasívne; • Kompatibilita so Switch CORE TYP1.
Príslušenstvo – napájací zdroj	• redundantný napájací zdroj – dva zdroje; • Kompatibilný so Switch CORE TYP 1; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 715 W.
Príslušenstvo – SFP+ modul	• 12 ks SPF+ modul; • Kompatibilita so Switch CORE TYP1.

Switch CORE časť - TYP 2 (2 ks)	
10/100/1000 porty	• 24x 1G metalické
Pamäť DRAM	• 8 GB
Pamäť flash	• 16 GB
Počet VLAN IDs	• 4094
Uplink konfigurácia	• Modulárna
Kapacita prepínania	• 208 Gbps
Stakovacia šírka pásma	• 688 Gbps
Rýchlosť preposielania	• 154,76 Mpps
Celový počet MAC adries	• 32 000
IPv4 direct routes	• 24 000
IPv4 indirect routes	• 8 000
IPv6 routes	• 16 000
Rozsah multicast routing	• 8 000
Rozsah QoS záznamov	• 5 120
Rozsah ACL záznamov	• 5 120
Jumbo ethernet rámce	• 9198 bajtov
Príslušenstvo – stohovací kábel 2	• 2ks stohovací kábel; • Kompatibilný so Switch CORE TYP 2; • Možnosť sériového napájania zariadení; • Dĺžka 1,5 m.
Príslušenstvo – sieťový modul	• 10 GE SFP+; • Rýchlosť 1G/10Gb/s; • Chladenie pasívne; • Kompatibilita so Switch CORE TYP2.
Príslušenstvo – napájací zdroj	• Redundantný napájací zdroj - dva zdroje; • Kompatibilný so Switch CORE TYP 2; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 350 W.

Switch CORE časť - TYP 3 (1 ks)	
10/100/1000 porty	• 24
Pamäť DRAM	• 2 GB
Pamäť flash	• 4 GB
Počet VLAN IDs	• 4096
Kapacita prepínania	• 128 Gbps
Stakovacia šírka pásma	• 80 Gbps
Rýchlosť preposielania	• 95,23 Mpps
Celkový počet MAC adries	• 16 000
IPv4 direct routes	• 8 000
IPv4 indirect routes	• 3 000
IPv6 routes	• 1 500
Rozsah multicast routing	• 1 000
Rozsah QoS záznamov	• 1 000
Rozsah ACL záznamov	• 1 500
Jumbo ethernet rámce	• 9 198 bajtov
Príslušenstvo – napájací zdroj	• redundantný napájací zdroj – dva zdroje; • Kompatibilný so Switch CORE TYP 3; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 125 W.

Router CORE časť - TYP 1 (2 ks)	
10/100/1000 porty	• 24x 1G SFP
Pamäť DRAM	• 4 GB
Pamäť flash	• 2 GB
Ethernet LAN	• Áno
Podpora L2 VPN	• Áno
Podpora L3 VPN	• Áno
Rýchlosť prenosu	• 1 000, 10 000 Mbit/s
Podpora QoS	• Áno
Príslušenstvo – SFP+ modul	• 2 ks SPF+ modul; • Kompatibilita so Router časť CORE TYP1.

Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete

Autentifikátor

- Počet užívateľov: 700;
- Počet mobilných SW tokenov: 650;
- Počet HW tokenov: 50;
- Počet užívateľských certifikátov: 700;
- Nasadenie vo VM úspešného poskytovateľa;
- Podpora hypervízorov: VMware ESXi/ ESX 6ú7/8, Microsoft Hyper-V Server 2010, 2012 RC a 2016, KVM, Xen, Microsoft Azure, AWS, Nutanix AHV, Oracle OCI, Alibaba Cloud;
- Podpora režimu vysokej dostupnosti („HA“);
- Možnosť upgrade licencie min. na dvojnásobok voči požadovanej kapacite;

Mobilný SW token / HW token

- V prípade SW tokenu, mobilná aplikácia kompatibilná s mobilnými zariadeniami iOS, Android, Windows;
- V prípade HW tokenu – prenosné zariadenie napr. vo forme kľúčenky.
- Požadovaný počet licencií pre koncové zariadenia: 700;
- inštalácia na mobilné zariadenia Verejného obstarávateľa (v prípade SW tokenu);
- funkcionalita generovania jednorazového hesla;
- dynamické generovanie hesiel;
- kompatibilita s ponúknutým VPN klientom a jestvujúcou infraštruktúrou Verejného obstarávateľa;
- overovanie užívateľov musí služba zabezpečovať prostredníctvom samostatného autentifikačného servera;
- podpora time-based ako aj event-based tokenov;
- kompatibilita s OATH.

VPN KLIENT

- Počet užívateľov: 700;
- Inštalácia na zariadenia Verejného obstarávateľa;
- Možnosť konfigurácie zero trust pravidiel prístupu do siete;
- Možnosť centrálneho manažmentu;
- Centralizované logovanie a reporting;
- Podpora IPSEC VPN a SSL VPN s viacfatorovým overením (podpora mobilného SW tokenu – kompatibilita s navrhovaným riešením Uchádzača);
- Podpora webfilteringu;
- Podpora výrobcu 24/7;
- On premise inštalácia;
- Jednoduché a prehľadné užívateľské prostredie;
- Podpora integrácie na Active Directory;
- Dynamické riadenie prístupu;
- Podpora užívateľských skupín;
- Podpora dynamickej voľby brány.

Manažment koncových zariadení

- Funkcionalita manažmentu koncových zariadení;
- Požaduje sa nasadenie v infraštruktúre dodávateľa;
- Podpora vzdialenej správy VPN klientov;
- Možnosť priraďovania bezpečnostných profilov pre skupiny koncových zariadení;
- podpora nasadzovania VPN klientov;
- správa aktualizácií a verzií VPN klientov;
- užívateľský dashboard;
- možnosť integrácie na Active Directory;
- automatické generovanie definovaných alertov;
- centralizovaný provisioning užívateľov;
- možnosť centralizovaného update VPN klientov;
- možnosť centralizovanej správy užívateľských skupín;

- funkcionalita karantény koncových zariadení;
- automatizovaný monitoring koncových zariadení (verzie, OS IP/MAC adresy, stav koncových zariadení).

Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

Platforma pre centralizovanú ochranu a správu 700 ks koncových staníc	
Centrálna správa a manažment koncových zariadení	• jednoduché používateľské grafické rozhranie centralizovaného manažmentu; • možnosť diaľkového nasadenia klientov na koncové zariadenia; • údaje o prevádzke na koncovej stanici zobrazované v reálnom čase; • integrácia na Active Directory; • centrálna správa karantény; • možnosť priraďovania koncových zariadení do skupín; • automatizované notifikácie; • centralizovaný provisioning klientov; • automatické reakcie systému na hrozby; • možnosť centralizovaného SW na koncovej stanici; • ochrana SSL VPN klienta;
Telemetria a monitoring koncových zariadení	• informácie a klientovi na koncovej stanici (verzia, OS, IP/MAX adresa, profil užívateľa); • stav klientskej stanice; • možnosť reportovania telemetrie na úrovni centrálnej správy;
Kompatibilita riešenia pre koncové stanice	• MS Windows, MacOS, iOS, Linux.

5.1 Prehľad e-Government komponentov

n/a

6. LEGISLATÍVA

Na dosiahnutie cieľov projektu nie je potrebná zmena legislatívy.

Projekt má za účel zosúladiť existujúci stav s právnymi predpismi:

- 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 NIS2,
- 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. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2003 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy

7. ROZPOČET A PRÍNOSY

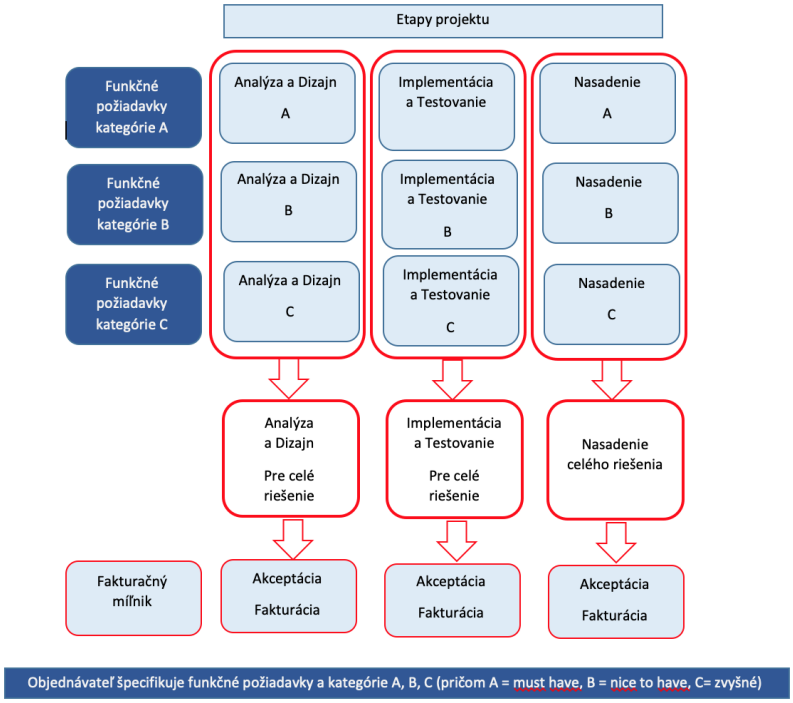
7.1 Sumarizácia nákladov a prínosov

Náklady (EUR s DPH)	**Modul: Audit bezpečnosti a hodnotenie rizík**	**Modul: Dokumentácia a politiky bezpečnosti**	**Modul : Správa prístupov koncových zariadení**	**Modul: Segmentácia siete a zabezpečenie komunikácie**	**Modul: Dodávka aktívnych prvkov siete**	**Modul: Dvojfaktorová autentifikácia**	**Modul: Centrálny bezpečnostný manažment**
Všeobecný materiál							
IT - CAPEX							
Aplikácie			*37.760,00*				*28.160,00*
SW						*31.632,00*	
HW			*8.372,00*		*121.164,00*	*2.498,00*	
Jednorazové činnosti expertov s dodaním diela	*8.500,00*	*60.360,00*	*18.340,00*	*36.404,00*	*18.340,00*	*11.160,00*	*11.200,00*

Náklady (EUR s DPH)	Modul: Audit bezpečnosti a hodnotenie rizík	Modul: Dokumentácia a politiky bezpečnosti	Modul : Správa prístupov koncových zariadení	Modul: Segmentácia siete a zabezpečenie komunikácie	Modul: Dodávka aktívnych prvkov siete	Modul: Dvojfaktorová autentifikácia	Modul: Centrálny bezpečnostný manažment
IT - OPEX- prevádzka							
Aplikácie							*1.465,00*
SW			*330,00*			*130,00*	
HW			*500,00*				
Prínosy							
Finančné prínosy							
Administratívne poplatky	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Ostatné daňové a nedaňové príjmy	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Ekonomické prínosy							
Občania (€)	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Úradníci (€)	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Úradníci (FTE)	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Kvalitatívne prínosy							

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU A METÓDA JEHO RIADENIA

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	*Prípravná fáza*	*02/2024*	*04/2024*	
2.	*Iniciačná fáza*	*08/2024*	*12/2024*	
3.	*Realizačná fáza*	*01/2025*	*12/2025*	
3a	*Analýza a dizajn*	*01/2025*	*03/2025*	
3b	*Nákup HW/SW*	*01/2025*	*12/2025*	
3c	*Implementácia a testovanie*	*04/2025*	*10/2025*	
3d	*Nasadenie*	*11/2025*	*12/2025*	
4.	*Dokončovacia*	*01/2026*	*02/2026*	
5.	*Podpora prevádzky SLA*	*03/2026*	*02/2031*	*5 rokov udržateľnosť (60 mesiacov)*



Pre tento projekt sa plánuje riadenie systémom „WATERFALL", ktorý sa javí ako vhodnejšia alternatíva k agilnému prístupu, nakoľko všetky projektové etapy bude pomerne jednoznačne možné identifikovať, ohraničiť a realizovať vo vzťahu k ich vecnej a časovej závislosti. V rámci ďalších fáz projektu, predovšetkým v Iniciačnej fáze budú bližšie špecifikované jednotlivé etapy projektu a súslednosť pracovných balíkov „WPs" a to v súlade s metodikou riadenia projektov PRINCE2.

Projekt bude teda nasledovať metódu Waterfall s dôkladnými logickými prepojeniami medzi jednotlivými modulmi, ktoré budú realizované na základe funkčnej a technickej špecifikácie pripravenej v rámci prípravy projektu. Tento rozhodnutý prístup vyplýva z potreby vykonávať opatrenia v kybernetickej bezpečnosti (KIB) v úzkej súvislosti, no v správnom poradí. Hoci niektoré aktivity môžu prebiehať súčasne a môžu byť vykonávané rôznymi tímami, dodržiavať budú predom stanovenú stratégiu a celkový plán projektu. Vzhľadom na potrebu realizácie projektu v kontinuálnej prevádzke základných služieb mesta, nie je vhodné zvoliť agilný prístup k realizácii tohto plánu.

9. PROJEKTOVÝ TÍM

Riadiaci výbor

Riadiaci výbor je orgán zriadený Mestom Banská Bystricia. Riadiaci výbor je najvyšší riadiaci a kontrolný orgán projektu. Riadiaci výbor tvorí predseda riadiaceho výboru a ostatní členovia. Riadiaci výbor sa riadi Štatútom Riadiaceho výboru, ktorý upravuje najmä jeho pôsobnosť, úlohy, zloženie, zasadnutie a hlasovanie. Členom riadiaceho výboru projektu môže byť aj zástupca dodávateľa. Väčšina členov riadiaceho výboru projektu s hlasovacím právom sú osoby navrhnuté Mestom zastupujú záujmy Mesta ako objednávateľa. Riadiaci výbor projektu dozerá na hospodárnosť, efektívnosť a účelové využívanie finančných prostriedkov a môže prispôsobiť štandardy projektového riadenia na realizovaný projekt.

Riadiaci výbor projektu tvoria minimálne 3 členovia, vrátane predsedu Riadiaceho výboru.

Riadiaci výbor (RV), v minimálnom zložení:

- predseda riadiaceho výboru,
- zástupca kľúčových používateľov objednávateľa,
- zástupca dodávateľa (doplní sa až po VO).

Riadiaci výbor je riadený predsedom, ktorým je zástupca Mesta Banská Bystrica. V prípade neprítomnosti predsedu na zasadnutí Riadiaceho výboru, predseda musí na toto konkrétne zasadnutie písomne delegovať svoju funkciu v rozsahu svojich práv a povinností formou splnomocnenia na zástupcu, ktorým môže byť aj iný člen Riadiaceho výboru s hlasovacím právom, prípadne iná splnomocnená osoba.

Riadiaci výbor zasadá pravidelne, najmenej jedenkrát za dva (2) po sebe nasledujúce kalendárne mesiace. Zasadnutie Riadiaceho výboru zvoláva predseda. Zasadnutie Riadiaceho výboru vedie predseda, prípadne ním určený zástupca, na ktorého predseda na dané zasadnutie písomne delegoval svoju funkciu, alebo ten člen Riadiaceho výboru, ktorý požiadal o zasadnutie Riadiaceho výboru.

Hlavné dokumenty spojené s činnosťou Riadiaceho výboru sú program zasadnutia, pracovný materiál a záznam zo zasadnutia Riadiaceho výboru, ktorého prílohou musí byť aj prezenčná listina, prípadne aj písomné splnomocnenia členov Riadiaceho výboru. Závery zo zasadnutia Riadiaceho výboru a jednotlivé body zo zasadnutia Riadiaceho výboru sa prijímajú súhlasným hlasovaním nadpolovičnej väčšiny prítomných členov Riadiaceho výboru s hlasovacím právom. Hlas predsedu má v prípade rovnosti hlasov hodnotu dvoch hlasov.

Každý člen Riadiaceho výboru ma tieto práva a povinnosti:

a) právo a povinnosť zúčastňovať sa na zasadnutiach Riadiaceho výboru,
b) právo uplatniť si pripomienky, podávať podnety alebo vyjadriť sa k pracovnému materiálu predloženému na zasadnutí Riadiaceho výboru alebo v rámci dištančného hlasovania, ak sa jedná o člena Riadiaceho výboru s hlasovacím právom,
c) právo podávať návrhy a podnety týkajúce sa činnosti Riadiaceho výboru,
d) právo nahliadať do projektovej dokumentácie,
e) navrhovať zmeny Štatútu,
f) iné práva v zmysle tohto Štatútu a Projektového iniciálneho dokumentu (PID).

Člen Riadiaceho výboru zachováva mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedel pri výkone svojej funkcie alebo v súvislosti s ňou a ktoré v záujme Riadiaceho výboru nemožno oznamovať tretím osobám, a to aj po ukončení realizácie projektu.

Riadiaci výbor sa zriaďuje na účely realizácie projektu a bude zostavený v zložení:

ID	Meno a Priezvisko	Pozícia	Subjekt
1.	TBD	Predseda RV	Mesto Banská Bystrica
3.	TBD	Kľúčový používateľ	Mesto Banská Bystrica
7.	TBD	Zástupca Zhotoviteľa	TBD

Podrobná štruktúra RVP bude definovaná v rámci projektového iniciálneho dokumentu („PID“) v súlade s metodikou riadenia projektov PRINCE2®.

Projektový tím

Riadenie projektu zo strany Objednávateľa bude zabezpečené prostredníctvom Projektového manažéra a Finančného manažéra a bude trvať počas celej doby realizácie projektu. Bude pokrývať oblasť projektového riadenia (projektový manažment, celková koordinácia projektu, celkový dohľad nad dodávkou dodávaného Diela, vrátane kvality), finančného riadenia a monitorovania realizácie projektu v zmysle riadenia podľa Vyhlášky č. 401/2022 Z. z. v platnom znení.

Projektový tím bude pozostávať z pozícií:

i) Povinné projektové role:

- Projektový manažér objednávateľa;
- Kľúčový používateľ;
- IT architekt;
- Vlastník procesov;
- Manažér kybernetickej a informačnej bezpečnosti;
- Projektový manažér zhotoviteľa;
- Špecialista pre bezpečnosť IT;
- IT analytik;
- Špecialista pre infraštruktúrny/HW špecialista;
- IT/IS konzultant;
- IT tester;
- Školiteľ pre IT systémy.

iii) Ďalšie projektové role:

- Finančný manažér,

Projektový manažér Objednávateľa bude zabezpečovať koordináciu projektových činností a manažment v súlade s metodikou PRINCE2 (hlavné dokumenty, priebežné manažérske výstupy, a pod.). Projektový manažér Objednávateľa bude riadiť, administratívne a organizačne zabezpečovať implementáciu projektu, komunikovať s dodávateľmi, sledovať plnenie harmonogramu projektu a zabezpečovať dokumenty požadované MIRRI. Zároveň bude v spolupráci s projektovým manažérom dodávateľa koordinovať realizáciu hlavných aktivít, činností a úloh projektu. Zodpovednosťou projektového manažéra je v spolupráci s finančným manažérom (objednávateľa) finančné riadenie projektu kontrolu rozpočtu projektu a jeho súlad s účtovnými dokladmi. Kontrolu podpornej účtovnej dokumentácie a poradenstvo pri definovaní oprávnených výdavkov bude zabezpečovať finančný manažér Objednávateľa.

Súčasťou projektovej kancelárie a projektového riadenia bude tiež operatívna projektová podpora zabezpečujúca administratívnu podporu pre písomnú komunikáciu, administratívne vedenie projektovej dokumentácie a prípravu podkladov pre členov projektového tímu, organizáciu stretnutí a pod.. V rámci aktivity budú taktiež zabezpečovaný manažment a hodnotenie kvality zo strany Objednávateľa.

ID	Meno a Priezvisko	Pozícia	Organizačný útvar	Rola v projekte
1.	TBD	TBD	TBD	Projektový manažér
2.	TBD	TBD	TBD	Kľúčový používateľ
3.	TBD	TBD	TBD	IT architekt
4.	TBD	TBD	TBD	Vlastník procesov
5.	Ing. Bibiána Palušková	Manažér IB a KB	PR-MKB	Manažér kybernetickej a informačnej bezpečnosti
6.	TBD	TBD	TBD	Projektový manažér zhotoviteľa
7.	TBD	TBD	TBD	Špecialista pre bezpečnosť IT
8.	TBD	TBD	TBD	IT analytik
9.	TBD	TBD	TBD	Manažér kvality
10.	TBD	TBD	TBD	IT/IS konzultant
11.	TBD	TBD	TBD	IT tester
12.	TBD	TBD	TBD	Školiteľ pre IT systémy
13.	TBD	TBD	TBD	Finančný manažér

10. ODKAZY

n/a

11. PRÍLOHY

Príloha 1: Zoznam rizík a závislosti
Príloha 2: Katalóg požiadaviek