PRÍSTUP K PROJEKTU

Povinná osoba	Mesto Ružomberok
Názov projektu	Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok
Zodpovedná osoba za projekt	PhDr. Vladimíra Pazderová, PhD.
Realizátor projektu	Mesto Ružomberok
Vlastník projektu	Mesto Ružomberok

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	PhDr. Vladimíra Pazderová, PhD.	Novo Funding	Projektový manažér	14.6.2024	
Schválil	Ing. Martin Žabenský	Mesto Ružomberok	Vedúci oddelenia informačných technológií	21.6.2024	

1. HISTÓRIA DOKUMENTU

Verzia	**Dátum**	**Zmeny**	**Meno**
1.0	14.6.2024	Prvá verzia dokumentu	PhDr. Vladimíra Pazderová, PhD.
1.1	21.6.2024	Finálna verzia dokumentu	PhDr. Vladimíra Pazderová, PhD.

2. ÚČEL DOKUMENTU

V súlade s Vyhláškou 401/2023 Z.z. dokument popisuje nasledovné oblasti:

- Opis navrhovaného riešenia
- Architektúra riešenia projektu na úrovni biznis vrstvy
- Architektúra riešenia projektu na úrovni aplikačnej vrstvy
- Architektúra riešenia projektu na úrovni dátovej vrstvy
- Architektúra riešenia projektu na úrovni technologickej vrstvy
- Infraštruktúra navrhovaného riešenia
- Bezpečnostná architektúra
- Špecifikácia údajov spracovaných v projekte, čistenie údajov
- Závislosti na ostatné IS/Projekty
- Zdrojové kódy
- Prevádzka a údržba výstupov projektu
- Požiadavky na personál
- Implementácia a preberanie výstupov projektu

Dokument rozpracováva detailné informácie v rámci prípravy projektu z pohľadu aktuálneho stavu, budúceho stavu a navrhovaného riešenia.

2.1 Použité skratky a pojmy

SKRATKA/POJEM	**POPIS**
KIB	Kybernetická a informačná bezpečnosť
SIEM	Security Information and Event Management
SOC	Security Operations Center
IS	Informačný systém
SLA	Service Desk Manager
SW	Softvér

MsÚ	Mestský úrad
ISVS	Informačný systém verejnej správy
MCA	Multikriteriálna analýza
PZS	Poskytovateľ základnej služby
NKIVS	Národná koncepcia informatizácie verejnej správy

2.2 Konvencie pre typy požiadaviek (príklady)

Na označenie čísla položky sa v dokumente používa prefix ID a poradové číslo položky.

3. POPIS NAVRHOVANÉHO RIEŠENIA

Projekt "Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok" je zameraný na zásadné zlepšenie ochrany informačných systémov a infraštruktúry. Tento projekt je navrhnutý tak, aby reagoval na súčasné a budúce bezpečnostné výzvy, pričom zároveň zabezpečuje súlad s legislatívnymi požiadavkami a normami v oblasti kybernetickej bezpečnosti.

Biznis architektúra projektu definuje kľúčové biznis procesy, ktoré budú optimalizované a chránené prostredníctvom technologických a organizačných opatrení. Tieto procesy zahŕňajú detekciu a reakciu na bezpečnostné incidenty, správu a analýzu dát, ako aj vzdelávanie a školenie zamestnancov. Cieľom je dosiahnuť vysokú úroveň ochrany dát, zabezpečenie nepretržitej dostupnosti služieb a posilnenie kybernetickej odolnosti mesta.

Aplikačná architektúra sa zameriava na implementáciu a integráciu pokročilých bezpečnostných systémov, ako sú SIEM a NGFW, ktoré sú kľúčové pre monitorovanie, analýzu a reakciu na bezpečnostné hrozby. Tieto systémy budú integrované s existujúcimi IT systémami mesta a poskytnú centralizovaný prehľad o bezpečnostnom stave a rýchlu reakciu na incidenty.

Technologická architektúra obsahuje modernizáciu fyzickej a sieťovej infraštruktúry, zahrňujúcu výmenu zastaraných komponentov, zavedenie a rozšírenie segmentácie siete. V rámci serverovej infraštruktúry bude vykonaná modernizácia serverov a zavedenie riešení pre vysokú dostupnosť a rýchlu obnovu systémov. Zálohovacie riešenia a pokročilé bezpečnostné nástroje zabezpečia ochranu kritických dát a systémov.

Tento projekt predstavuje komplexné riešenie kybernetickej a informačnej bezpečnosti, ktoré je navrhnuté tak, aby zodpovedalo najvyšším štandardom ochrany a efektivity. Zavedením moderných technológií a postupov sa výrazne zvýši úroveň bezpečnosti a zabezpečí kontinuita kritických služieb. Realizácia tohto projektu bude vyžadovať značné investície, avšak prínosy z hľadiska zvýšenej bezpečnosti a odolnosti sú neoceniteľné. Projekt je navrhnutý s ohľadom na budúce rozširovanie a prispôsobenie sa novým bezpečnostným výzvam, čo zabezpečí dlhodobú udržateľnosť a efektívnosť investícií.

Č.	Názov opatrenia	Popis	Výstup	Dopad/následok
1.	**Aktualizácia analýzy rizík**	Aktualizácia analýzy rizík zabezpečí správu aktív, zraniteľností, hrozieb a opatrení. Analýza rizík umožní aktualizovanie a hodnotenie rizík založené na aktuálnych dátach a poskytne nástroje pre efektívne riadenie a minimalizáciu rizík.	1. Aktualizácia analýzy rizík, hrozieb a zraniteľností, ktorej výsledky budú slúžiť ako východisko pre klasifikáciu informácií, kategorizáciu sietí a informačných systémov. 2. Aktualizácia klasifikácie informácií a kategorizácie sietí a informačných systémov, podľa klasifikačnej schémy v súlade s prílohou č.2 vyhlášky 362/2018.	*- zníženie zraniteľnosti vyplývajúcej s nedostatočného riadenie rizík a opatrení v oblasti KB*
2.	**Vybudovanie SIEM**	Monitorovanie hrozieb v reálnom čase prostredníctvom systémov ako SIEM, zabezpečí rýchlu reakciu na potenciálne bezpečnostné incidenty a výrazne prispieva k celkovej odolnosti mesta.	1. Implementácia SIEM 2. Dokumentácia a školenie.	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na neobvyklé udalosti)*
3.	**Vypracovanie a implementácia komplexného plánu kontinuity činností**	Vypracovanie a implementácia plánu kontinuity činností (BCM), ktorý zahŕňa postupy pre rýchlu obnovu kritických systémov a služieb po narušení. Plán bude obsahovať scenáre pre rôzne	1. Plán kontinuity činností musí obsahovať minimálne: a. Plán kontinuity na stanovenie požiadaviek a zdrojov b. Plán reakcie na incidenty a plány havarijnej obnovy prevádzky c. Politiku a ciele kontinuity d. Analýzu funkčných	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na neobvyklé udalosti)*

		typy udalostí a zahrnie analýzu funkčných dopadov, strategické zdroje na obnovu a časové rámce pre reakciu.	dopadov e. Stratégiu riadenia kontinuity vrátane evakuačných postupov f. Plán údržby a kontroly BCMS. 2. Školenie	
4.	**Modernizácia sieťovej infraštruktúry v mestskej informačnej sieti**	Zabezpečí sa výmena zastaraných sieťových prvkov, dobudovanie záložných trás a rozšírená segmentácia siete. Tieto kroky významne prispejú k zníženiu zraniteľností vyplývajúcich z používania EOL zariadení a ich nedostatočného zabezpečenia.	1. Vstupná analýza existujúcej sieťovej infraštruktúry a návrhu opatrení v zmysle vyhlášky NBU č.362/2018. 2. Výmena a inštalácia zastaralých sieťových prvkov na úrovni L2/L3. 3. Rekonfigurácia siete vrátane rozšírenej segmentácie a rozdelenia na VLAN. 4. Vytvorenie alebo aktualizácia dokumentácie počítačovej siete, ktorá obsahuje evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov 5. Zaškolenie IT personálu	*- zníženie zraniteľnosti vyplývajúcej z použitia EOL zariadení (nedostatočné zabezpečenie)* *- zníženie zraniteľnosti vyplývajúcej nízkej dostupnosti poskytovania základnej služby.*
5.	**Modernizácia serverovej infraštruktúry**	Výmena serverových komponentov, sieťových prvkov prispeje k zníženiu rizika nízkej dostupnosti poskytovania základnej služby a zraniteľnosti spojenej s používaním zastaraných zariadení.	1. Výmena serverov. 2. Výmena sieťových prvkov pre iSCSI. 3. Nasadenie platformy pre beh VM 4. Kompletná konfigurácia, dokumentácia a , zaškolenie IT pracovníkov 5. Montáž, inštalácia serverov a storage a ich prepojenie, nastavenie Domény, konfigurácia Active Directory, migrácia dát a migrácia databáz. 6. Aktualizácia, vypracovanie a dodanie príslušnej systémovej a používateľskej dokumentácie k vykonaným zmenám 7. Zaškolenie IT personálu	*- zníženie zraniteľnosti vyplývajúcej z použitia EOL zariadení (nedostatočné zabezpečenie)* *- zníženie zraniteľnosti vyplývajúcej nízkej dostupnosti poskytovania základnej služby.*
6.	**Zavedenie a správa nástroja na riadenie kapacít**	Nástroj na riadenie kapacít umožní nepretržité sledovanie všetkých IT aktív, poskytovanie včasných upozornení na potenciálne problémy a umožní rýchlu reakciu na incidenty. Týmto spôsobom sa zlepší viditeľnosť a kontrolu nad IT infraštruktúrou, čím sa zabezpečí jej spoľahlivú a bezpečnú prevádzku.	1. Inštalácia a základná konfigurácia. 2. Nastavenie monitorovacích objektov. 3. Konfigurácia upozornení a eskalácií. 4. Vizuálne rozhrania a reporty 5. Integrácia a rozšírenia. 6. Bezpečnosť a prístupové práva. 7. Školenie a podpora.	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na neobvyklé udalosti)*
7.	**Nastavenie zálohovania**	Zavedenie stratégie a plánov zálohovania zabezpečí zvýšenie dostupnosti základnej služby.	1. Analýza a plánovanie zálohovania 2. Konfigurácia zálohovacieho softvéru 3. Automatizácia a monitorovanie. 4. Testovanie a validácia zálohovania 5. Školenie a dokumentácia	*- zníženie zraniteľnosti vyplývajúcej s potencionálnej straty údajov (zlyhanie HW, ransomware atd.)*
8.	**Dodanie a**	Umožní pokročilé	Dodanie a implementácia next-gen firewall	– *zníženie zraniteľnosti*

	implementácia next-gen firewall technológie	filtrovanie obsahu, riadenie prestupov medzi sieťovými segmentami a integráciu s aktuálnymi bezpečnostnými systémami	technológie vrátane: 1. Analýza súčasného stavu 2. Návrh implementačného konceptu a dizajnu riešenia 3. Inštalácia nového HW v priestoroch objednávateľa 4. Základná konfigurácia FW (IP adresa, názov, zóny, manažment ....) 5. Vytváranie nových pravidiel podľa pripraveného konceptu 6. Konfigurácia VPN tunelov 7. Migrácia objektov, smerovania, NAT 8. Migrácia komunikačných pravidiel 9. Integrácia so všetkými prvkami sieťovej infraštruktúry 10. Testovanie riešenia v testovacom prostredí 11. Migrácia do produkčného prostredia 12. Vyriešenie komunikačných problémov (prepojenie na externé subjekty, portály a pod. 13. Z inštalácie a kompletnej konfigurácie zariadenia 14. Aktualizácia, vypracovanie a dodanie príslušnej systémovej a používateľskej dokumentácie k vykonaným zmenám 15. Zaškolenie IT personálu	– *vyplývajúcej z nedostatočnej kontroly obsahu, monitorovania a analýzy informácií (únik informácií z vnútra, bezpečnostné incidenty)* – *zníženie zraniteľnosti vyplývajúcej z potencionálnych sieťových útokov na infraštruktúru MsÚ (DDoS, password attack, spoofing, neautorizovaný prístup..)*
9.	**Vykonanie auditu kybernetickej bezpečnosti**	Vykonanie auditu a na začiatku a na konci projektu poskytne hodnotný prehľad o efektívnosti prijatých opatrení a pomôže identifikovať ďalšie možnosti zlepšenia.	1. Audit kybernetickej bezpečnosti v zmysle platného zákona o kybernetickej bezpečnosti. a. Vykonaný audit b. Záverečná správa o výsledkoch vykonaného auditu	- *vyhodnotenie dopadu prijatých opatrení na zvýšenie kybernetickej bezpečnosti*

4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

Opatrenia, ktoré sú predmetom projektu sú zamerané na zabezpečenie prevádzky základnej služby resp. zabezpečenie najmä dôvernosti, dostupnosti a integrity ako služby tak aj samotných informácií.

Na prevádzke danej základnej služby sa podieľajú tieto systémy:

- Informačný systém mesta ISS Cora Geo
- Dokumentačný informačný systém samosprávy Cora Geo DISS
- Mail server
- Web server - www.ruzomberok.sk

AS IS stav

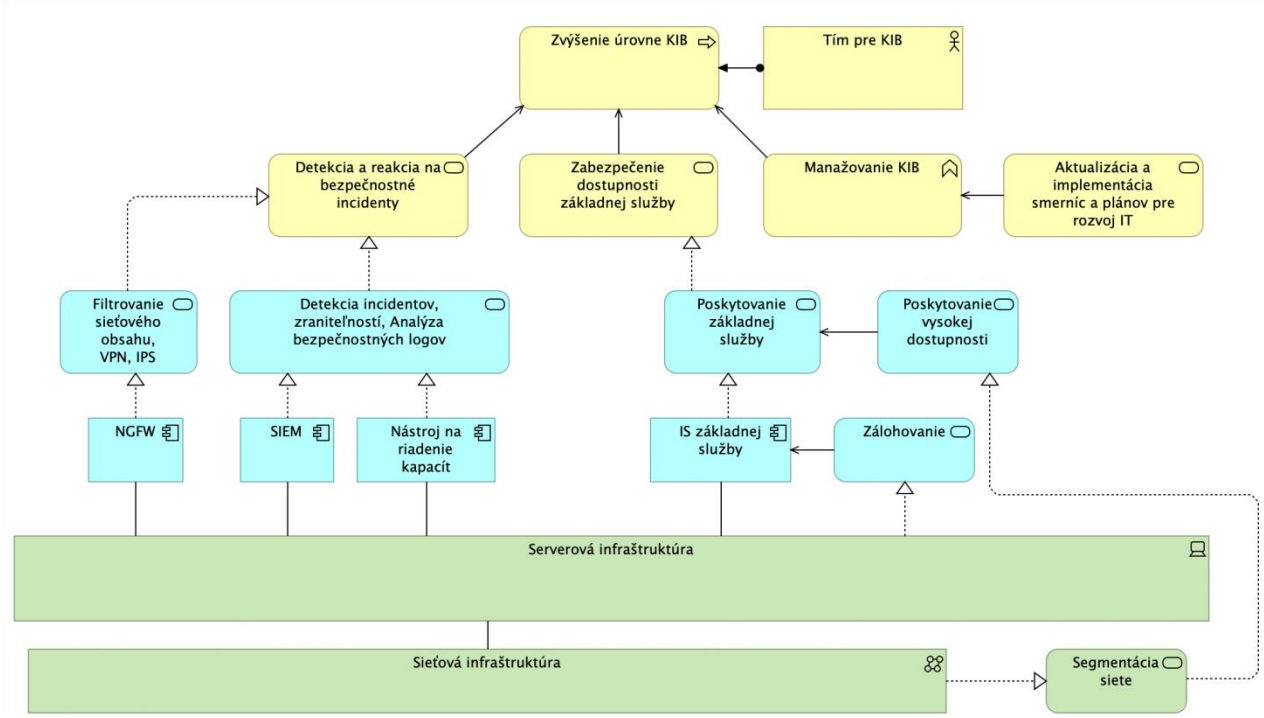
V súčasnom stave mesto Ružomberok prevádzkuje základné IT infraštruktúrne a bezpečnostné komponenty, ktoré zahŕňajú základnú sieťovú infraštruktúru a tradičné bezpečnostné riešenia bez integrácie pokročilých analytických nástrojov. Biznis procesy sú čiastočne digitalizované, avšak bez špecializovaných nástrojov pre detekciu a reakciu na kybernetické hrozby.

Aplikačná vrstva zahŕňa základné IT nástroje pre správu siete a bezpečnostných politík, avšak chýbajú integrované systémy pre centralizovanú správu bezpečnostných udalostí a údajov.

Technologická infraštruktúra zahŕňa zastarané servery a sieťové zariadenia, ktoré nepodporujú moderné bezpečnostné štandardy ani vysokú dostupnosť.

TO BE stav

- Biznis Architektúra - Nová biznis architektúra zahŕňa modernizované procesy s integráciou pokročilých bezpečnostných systémov a politík, ktoré posilňujú ochranu dát a zabezpečujú kontinuitu operácií.
- Aplikačná Architektúra - Aplikačná vrstva zavádza pokročilé systémy ako SIEM a NGFW, ktoré sú plne integrované pre efektívne monitorovanie a rýchlu reakciu na bezpečnostné incidenty.
- Technologická Architektúra - Modernizovaná technologická infraštruktúra zahŕňa najnovšie servery, sieťové zariadenia a zálohovacie systémy, ktoré zabezpečujú vysokú dostupnosť a rýchlu obnovu po incidentoch.



Obrázok 1 Architektúra TO BE stav

4.1 Biznis vrstva

AS IS stav

Mesto Ružomberok je ako poskytovateľ základných služieb zapísaný do registra PZS od 1.3.2020, pričom sa jedná o službu Správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. Informačné systémy mesta Ružomberok boli budované živelne, bez koncepcie, ktorej cieľom by bola kybernetická bezpečnosť, v dôsledku čoho sa témou stáva otázka zabezpečenia informačných aktív mesta Ružomberok, tak aby spĺňali požiadavky vyplývajúce vyplývajúce zo zákonov č. 69/2018 Z. z. a č. 95/2019 Z. z. a požiadavky na GDPR. Mesto Ružomberok si uvedomuje tiež narastajúci vplyv informačných systémov na chod úradu a úroveň služieb, ktoré poskytuje verejnosti. Rovnako citlivo vníma tiež informácie o rastúcom počte a závažnosti kybernetických incidentov. Práve s ohľadom na uvedené vykonalo prvý krok k zlepšeniu úrovne kybernetickej bezpečnosti v rámci identifikácie kritických oblastí a definovania opatrení potrebných na minimalizáciu rizík a dopadov v danej oblasti.

Mesto Ružomberok má formálne definovanú pozíciu Manažéra kybernetickej bezpečnosti, z ktorej vyplýva jeho možnosť predkladať návrhy a oznamovať informácie v oblasti KB priamo štatutárnemu orgánu PZS a jeho nezávislosť od riadenia prevádzky a vývoja služieb informačných technológií. Mesto využíva ako centrálny informačný systém podporujúci základnú službu informačný systém samosprávy CG ISS od dodávateľa CoraGeo. Jedná sa o komplexné, modulové softvérové vybavenie pre chod mestských a obecných úradov, ktorý pokrýva celú agendu úradu a odstraňuje duplicitu, keďže využíva iba jednu databázu. Informačná aplikácia pre obyvateľov mesta je webová stránka mesta.

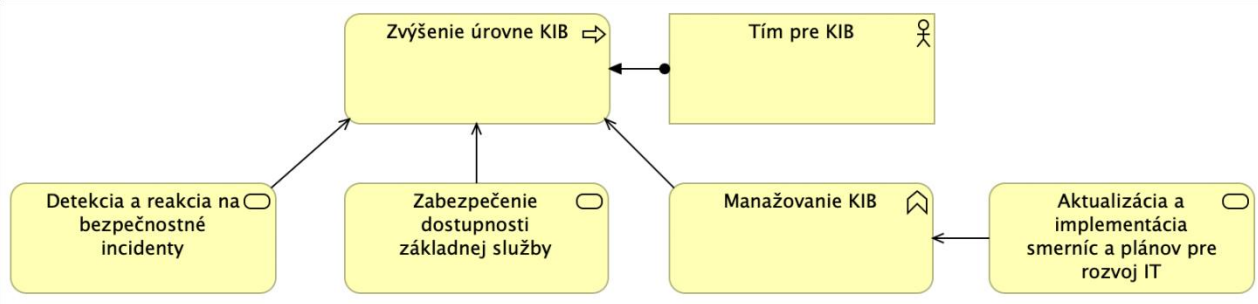
TO BE stav

Model architektúry zobrazujúci budúci stav biznis vrstvy architektúry pre mesto Ružomberok ilustruje komplexné a integrované riešenie KIB. Riešenie sa sústreďuje na zvýšenie odolnosti mesta voči bezpečnostným hrozbám prostredníctvom implementácie proaktívnych ochranných opatrení, zlepšeného monitorovania a správy bezpečnostných politík.

Hlavné biznis procesy, ktoré sú nevyhnutné pre zvýšenie úrovne KIB sú:

- Detekcia a reakcia na bezpečnostné incidenty zabezpečujúca neustále monitorovanie a rýchlu reakciu na akékoľvek potenciálne hrozby.
- Aktualizácia a implementácia smerníc a plánov pre rozvoj IT zaručujúca, že všetky bezpečnostné opatrenia sú aktuálne a v súlade s najnovšími štandardmi a praxami.
- Zabezpečenie dostupnosti základnej služby zaručujúcej že IS základnej služby a ich služby sú dostupné svojim používateľom

Architektúra zdôrazňuje dôležitosť tímu pre KIB, ktorý je zodpovedný za riadenie a vykonávanie bezpečnostných operácií. Manažér KIB a Bezpečnostný analytik spolupracujú na zabezpečení dostupnosti základných služieb a zabezpečení siete, pričom zároveň riadia aktualizácie a implementáciu smerníc a plánov pre rozvoj IT.



Obrázok 2 Model biznisovej architektúry TO BE stavu

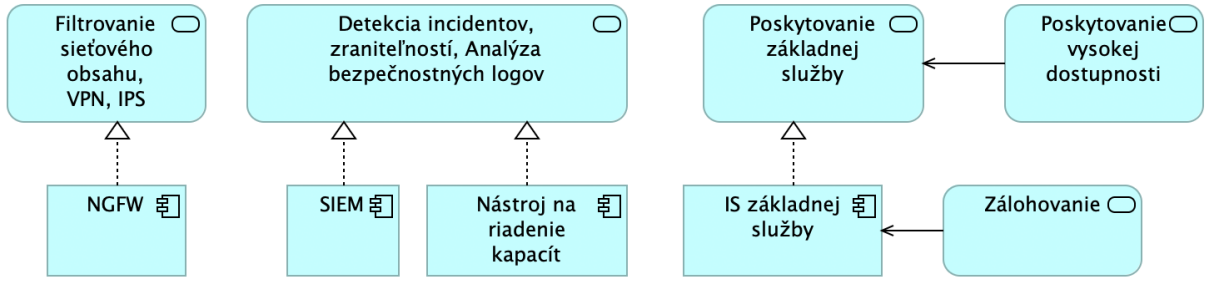
4.1.1 Prehľad koncových služieb – budúci stav:

V rámci projektu sa nerealizujú koncové služby ale opatrenia, ktoré okrem zvýšenia KIB v oblasti poskytovania základnej služby zvýšia aj KIB v oblasti poskytovania existujúcich koncových služieb mesta Ružomberok.

4.1.2 Jazyková podpora a lokalizácia

Dodávané riešenie musí mať Slovensku jazykovú lokalizáciu. Ďalšie lokalizácie nie sú požadované

4.2 Aplikačná vrstva



Obrázok 3 Model aplikačnej architektúry TO BE stavu

V aplikačnej vrstve sú implementované kľúčové technologické riešenia. Centrálnym prvkom aplikačnej architektúry je SIEM, ktorý slúži ako hlavný nástroj pre detekciu incidentov a analýzu bezpečnostných logov. Tento systém je zásadný pre identifikáciu a rýchlu reakciu na bezpečnostné udalosti, čím výrazne znižuje riziko a možné škody z bezpečnostných incidentov. NGFW zabezpečuje filtrovanie sieťového obsahu, VPN a IPS. Nástroj na riadenie kapacít zabezpečuje monitoring IT infraštruktúry.

Tieto systémy sú neoddeliteľne spojené s informačnými systémami základnej služby a spolu tvoria integrovanú súčasť poskytovania základných služieb mesta. Vysoká dostupnosť je zabezpečená modernizáciou na úrovni technologickej vrstvy v podobe nových serverov, sieťových komponentov a segmentácie. Tento prístup zaručuje, že základné služby mesta budú nepretržite dostupné aj v prípade neočakávaných udalostí.

Celkovo tieto prvky tvoria komplexný systém zameraný na prevenciu, odolnosť a reakciu na bezpečnostné výzvy.

4.2.1 Rozsah informačných systémov - AS IS

V nasledujúcej tabuľke uvádzame ISVS, ktoré zabezpečujú prevádzku základnej služby Mesta Ružomberok a budú chránené proti incidentom KIB po ukončení projektu:

Kód ISVS *(z MetaIS)*	**Názov ISVS**	**Modul ISVS** *(zaškrtnite ak ISVS je modulom)*	**Stav IS VS**	**Typ IS VS**	**Kód nadradeného ISVS** *(v prípade zaškrtnutého checkboxu pre modul ISVS)*
isvs_11416	Informačný systém mesta ISS Cora Geo	☐	Prevádzkovaný a plánujem rozvíjať	Integračný	
isvs_11317	Dokumentačný informačný systém samosprávy Cora Geo DISS	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	

Kód ISVS *(z MetaIS)*	**Názov ISVS**	**Modul ISVS** *(zaškrtnite ak ISVS je modulom)*	**Stav IS VS**	**Typ IS VS**	**Kód nadradeného ISVS** *(v prípade zaškrtnutého checkboxu pre modul ISVS)*
isvs_14332	Mail server	☐	Prevádzkovaný a neplánujem rozvoj	Ekonomický a adm. chod inštitúcie	
isvs_12794	Web server	☐	Prevádzkovaný a plánujem rozvíjať",	Prezentačný	

4.2.2 Rozsah informačných systémov - TO BE

V rámci projektu nevznikne nový ISVS v zmysle definície zákona o ISVS. Vznikne súbor opatrení, ktorý bude chrániť existujúce ISVS (ich zoznam viď predchádzajúca kapitola).

4.2.3 Využívanie nadrezortných a spoločných ISVS – AS IS

V rámci projektu nebudú využívané nadrezortné centrálne bloky.

4.2.4 Prehľad plánovaných integrácií ISVS na nadrezortné ISVS – spoločné moduly podľa zákona č. 305/2013 e-Governmente – TO BE

V rámci projektu nebudú využívané podporné spoločné moduly.

4.2.5 Prehľad plánovaného využívania iných ISVS (integrácie) – TO BE

V projekte neplánujeme integrácie na iné ISVS.

4.2.6 Aplikačné služby pre realizáciu koncových služieb – TO BE

V rámci projektu sa nerealizujú koncové služby ale opatrenia, ktoré okrem zvýšenia KIB v oblasti poskytovania základnej služby zvýšia aj KIB v oblasti poskytovania existujúcich koncových služieb mesta Ružomberok.

4.2.7 Aplikačné služby na integráciu – TO BE

V projekte neplánujeme integrácie na iné ISVS.

4.2.8 Poskytovanie údajov z ISVS do IS CSRÚ – TO BE

V rámci realizácie projektu neplánujeme poskytovanie údajov do IS CSRÚ.

4.2.9 Konzumovanie údajov z IS CSRU – TO BE

V rámci realizácie projektu neplánujeme konzumovanie údajov z IS CSRÚ.

4.3 Dátová vrstva

4.3.1 Údaje v správe organizácie

Projekt nebude priamo zabezpečovať správu údajov mesta Ružomberok, bude spravovať iba údaje nevyhnutné na zabezpečenie KIB mesta Ružomberok ako PZS. Z toho dôvodu neuvádzame namapovanú štruktúru údajov v správe Mesta Ružomberok.

4.3.2 Dátový rozsah projektu - Prehľad objektov evidencie - TO BE

V rámci realizovaného projektu nevzniknú nové objekty evidencie tak, ako vznikajú v prípade štandardných informačných systémov. Predmetom evidencie nebudú napríklad občania resp. informácie o nich atď. Systém bude viesť evidenciu prístupov a oprávnení, v rámci služby SIEM budú vznikať záznamy o incidentoch a tieto budú vyhodnocované a na základe nich budú prebiehať priamo reakcie na kybernetické incidenty - poskytovateľom služby SOC v súčinnosti so zástupcami mesta Ružomberok.

4.3.3 Referenčné údaje

V projekte nebudú vznikať údaje, ktoré by sa dali označiť ako referenčné.

4.3.4 Otvorené údaje

V projekte nebudú vznikať údaje, ktoré by mohli byť zverejnené ako otvorené.

4.3.5 Analytické údaje

V projekte nebudú vznikať údaje, ktoré by sa dali označiť ako analytické.

4.3.6 Moje údaje

V projekte nebudú vznikať údaje, ktoré by sa dali označiť ako moje údaje.

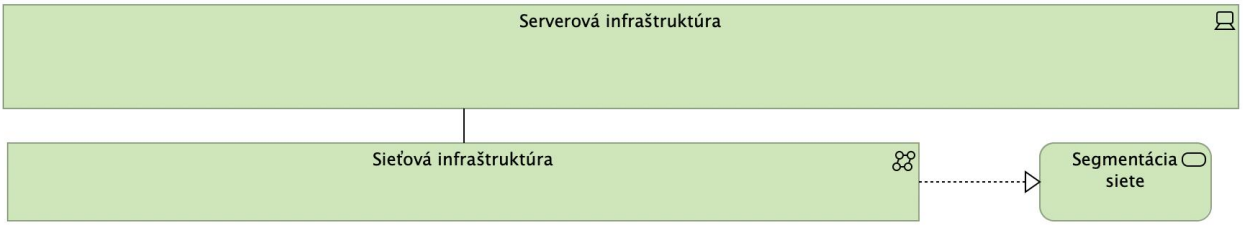
4.4 Technologická vrstva

AS IS stav

Sieťová infraštruktúra v mestskej informačnej sieti je tvorená zastaranými sieťovými prvkami, ktoré sú už v etape životného cyklu EOL (end of life) kedy už výrobca prestal dané zariadenie nielen vyrábať ale aj obmedzil ďalšiu podporu v podobe aktualizácii a bezpečnostných záplat. Rovnakým problémom trpí aj existujúca serverová infraštruktúra na ktorej sú prevádzkované aj IS poskytujúce základnú službu

TO BE stav

Základom tejto architektúry je serverová infraštruktúra, ktorá je kľúčová pre všetky IT operácie a služby. Sieťová infraštruktúra mesta je navrhnutá tak, aby bola odolnejšia a bezpečnejšia, s pokročilou segmentáciou, čo zvyšuje odolnosť proti bezpečnostným incidentom. Táto segmentácia umožňuje izoláciu a ochranu rôznych častí siete, čím sa minimalizuje riziko šírenia potenciálnych hrozieb a uľahčuje sa riadenie bezpečnostných politík.



Obrázok 4 Model technologickej architektúry TO BE stavu

Celkovo architektúra odráža záväzok mesta Ružomberok zabezpečiť, že jeho digitálna infraštruktúra je pripravená čeliť súčasným aj budúcim výzvam v oblasti IT bezpečnosti. S týmito krokmi sa mesto stavia do popredia pri zabezpečovaní a ochrane svojich občanov a ich dát, ako aj pri poskytovaní vysoko dostupných a spoľahlivých služieb.

4.4.1 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Parameter	Jednotky	Predpokladaná hodnota	Poznámka
Počet interných používateľov	Počet	276	
Počet súčasne pracujúcich interných používateľov v špičkovom zaťažení	Počet	100	
Počet externých používateľov (internet)	Počet	1000	odborný odhad
Počet externých používateľov používajúcich systém v špičkovom zaťažení	Počet	1000	odborný odhad
Počet transakcií (podaní, požiadaviek) za obdobie	Počet/obdobie	10000/rok	odborný odhad

4.4.2 Využívanie služieb z katalógu služieb vládneho cloudu

V realizovanom projekte neplánujeme využívať služby z katalógu vládneho cloudu.

4.5 Bezpečnostná architektúra

Dodávateľ sa zaviaže riešiť bezpečnostnú architektúru dodávaných IS,IKT a služieb v zmysle nasledujúcej legislatívy:

- Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe
- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Zákon č. 45/2011 Z.z. o kritickej infraštruktúre
- Vyhláška NBU č. 166/2018 Z.z., o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
- Vyhláška NBU č. 164/2018 Z.z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
- Vyhláška NBU č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Vyhláška NBU č. 436/2019 Z.z., o audite kybernetickej bezpečnosti a znalostnom štandarde audítora
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy
- 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 v

- Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

5. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

Realizovaný projekt nemá závislosti na iné projekty mesta.

6. ZDROJOVÉ KÓDY

Mesto Ružomberok plánuje pri obstarávaní postupovať v zmysle vzoru Zmluvy o dielo.

Zmluvnú úpravu predkladáme nasledujúcu:

- Zhotoviteľ je povinný pri akceptácii Informačného systému odovzdať Objednávateľovi funkčné vývojové a produkčné prostredie, ktoré je súčasťou Informačného systému.
- Zhotoviteľ je povinný pri akceptácii Informačného systému alebo jeho časti odovzdať Objednávateľovi Vytvorený zdrojový kód v jeho úplnej aktuálnej podobe, zapečatený, na neprepisovateľnom technickom nosiči dát s označením časti a verzie Informačného systému, ktorej sa týka. Za odovzdanie Vytvoreného zdrojového kódu Objednávateľovi sa na účely tejto Zmluvy o dielo rozumie odovzdanie technického nosiča dát Oprávnenej osobe Objednávateľa. O odovzdaní a prevzatí technického nosiča dát bude oboma Zmluvnými stranami spísaný a podpísaný preberací protokol.
- Informačný systém (Dielo) v súlade s Technickou špecifikáciou obsahuje od zvyšku Diela oddeliteľný modul (časť) vytvorený Zhotoviteľom pri plnení tejto Zmluvy o dielo, ktorý je bez úpravy použiteľný aj tretími osobami, aj na iné alebo podobné účely, ako je účel vyplývajúci z tejto Zmluvy o dielo (ďalej ako „Modul"). A to najmä pre modul Karta občana. Vytvorený zdrojový kód Informačného systému (s výnimkou Modulu) vrátane jeho dokumentácie bude prístupný v režime podľa § 31 ods. 4 písm. b) Vyhlášky č. 78/2020 (s obmedzenou dostupnosťou pre orgán vedenia a orgány riadenia v zmysle Zákona o ITVS – vytvorený zdrojový kód je dostupný len pre orgán vedenia a orgány riadenia). Pre zamedzenie pochybností uvádzame, že sa jedná len o zdrojový kód, ktorý Dodávateľ vytvoril, alebo pozmenil v súvislosti s realizáciou diela. Objednávateľ je oprávnený sprístupniť Vytvorený zdrojový kód okrem orgánov podľa predchádzajúcej vety aj tretím osobám, ale len na špecifický účel, na základe riadne uzatvorenej písomnej zmluvy o mlčanlivosti a ochrane dôverných informácií.
- Ak je medzi zmluvnými stranami uzatvorená SLA zmluva, od prevzatia Informačného systému sa prístup k vytvorenému zdrojovému kódu vo vývojovom a produkčnom prostredí, vrátane nakladania s týmto zdrojovým kódom, začne riadiť podmienkami dohodnutými v SLA zmluve.
- Vytvorený zdrojový kód musí byť v podobe, ktorá zaručuje možnosť overenia, že je kompletný a v správnej verzii, t. j. v takej, ktorá umožňuje kompiláciu, inštaláciu, spustenie a overenie funkcionality, a to vrátane kompletnej dokumentácie zdrojového kódu (napr. interfejsov a pod.) takejto Informačného systému alebo jeho časti. Zároveň odovzdaný vytvorený zdrojový kód musí byť pokrytý testami (aspoň na 90%) a dosahovať rating kvality (statická analýza kódu) podľa CodeClimate/CodeQLa pod. (minimálne stupňa B).
- Pre zamedzenie pochybností, povinnosti Zhotoviteľa týkajúce sa Vytvoreného zdrojového kódu platí i na akékoľvek opravy, zmeny, doplnenia, upgrade alebo update Vytvoreného zdrojového kódu a/alebo vyššie uvedenej dokumentácie, ku ktorým dôjde pri plnení tejto Zmluvy o dielo alebo v rámci záručných opráv. Vytvorené zdrojové kódy budú vytvorené vyexportovaním z produkčného prostredia a budú odovzdané Objednávateľovi na elektronickom médiu v zapečatenom obale. Zhotoviteľ je povinný umožniť Objednávateľovi pri odovzdávaní Vytvoreného zdrojového kódu, pred zapečatením obalu, skontrolovať v priestoroch Objednávateľa prítomnosť Vytvoreného zdrojového kódu na odovzdávanom elektronickom médiu.
- Nebezpečenstvo poškodenia zdrojových kódov prechádza na Objednávateľa momentom prevzatia Informačného systému alebo jeho časti, pričom Objednávateľ sa zaväzuje uložiť zdrojové kódy takým spôsobom, aby zamedzil akémukoľvek neoprávnenému prístupu tretej osoby. Momentom platnosti SLA zmluvy umožní Objednávateľ poskytovateľovi, za predpokladu, že to je nevyhnutné, prístup k Vytvorenému zdrojovému kódu výlučne na účely plnenia povinností z uzatvorenej SLA zmluvy.

Následne ustanovenia predchádzaniu vendor-lockinu budú byť zahrnuté aj v ZoD a SLA.

Usmernenia pre oblasť zdrojových kódov:

- Metodické usmernenie č. 024077/2023 – o kvalite zdrojových kódov a balíkov softvéru zverejnené na stránke: https://mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/
- Inštrukcie k EUPL licenciám: https://commission.europa.eu/content/european-union-public-licence_en

7. PREVÁDZKA A ÚDRŽBA

Požadované SLA na služby systémovej a aplikačnej podpory – servisné služby vzťahujúce sa na produkčné a testovacie prostredie IS

Úrovne podpory používateľov:

Help Desk bude realizovaný cez 3 úrovne podpory, s nasledujúcim označením:

- **L1 podpory IS** (Level 1, priamy kontakt zákazníka) - jednotný kontaktný bod verejného obstarávateľa
- **L2 podpory IS** (Level 2, postúpenie požiadaviek od L1) - vybraná skupina garantov, so znalosťou IS (zabezpečuje prevádzkovateľ IS – verejný obstarávateľ).
- **L3 podpory IS** (Level 3, postúpenie požiadaviek od L2) - na základe zmluvy o podpore IS (zabezpečuje úspešný uchádzač).

Definícia:

Podpora L1 (podpora 1. stupňa) - začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.

Podpora L2 (podpora 2. stupňa) – riešiteľské tímy s hlbšou technologickou znalosťou danej oblasti. Riešitelia na úrovni Podpory L2 nekomunikujú priamo s koncovým užívateľom, ale sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát odovzdaných riešiteľmi 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách Objednávateľa. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať Hlásenie čo najskôr pod kontrolu a následne ho vyriešiť - s možnosťou eskalácie na vyššiu úroveň podpory – Podpora L3.

Podpora L3 (podpora 3. stupňa) - Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie tých najobtiažnejších hlásení, vrátane vykonávania hĺbkových analýz a riešenie extrémnych prípadov.

Riešenie incidentov – SLA parametre

Za incident je považovaná chyba IS, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou IS. Za incident nie je považovaná chyba, ktorá nastala mimo prostredia IS napr. výpadok poskytovania konkrétnej služby.

Označenie závažnosti incidentu:

Závažnosť incidentu	**Popis naliehavosti incidentu**
Kritická, Bezpečnostná	Kritické chyby, ktoré spôsobia úplné zlyhanie systému ako celku a nie je možné používať ani jednu jeho časť, nie je možné poskytnúť požadovaný výstup z IS.
Bežná	Chyby a nedostatky, ktoré spôsobia čiastočné obmedzenia používania systému.
Nekritická	Kozmetické a drobné chyby.

Vyžadované reakčné doby:

Označenie závažnosti incidentu	**Reakčná doba(1) od nahlásenia incidentu po začiatok riešenia incidentu**	**Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI) (2)**	**Spoľahlivosť (3)** (počet incidentov za mesiac)
Bežná	Do 24 hodín	48 hodín	5
Kritická	Do 12 hodín	24 hodín	3
Nekritická	Do 48 hodín	Vyriešené a nasadené v rámci plánovaných aktualizácií	5
Bezpečnostná	Do 12 hodín	24 hodín	3

- Požiadavky na hlásenie Incidentov sa spracúvajú v rámci časového pokrytia od 8:00 do 16:00.
- (1) Reakčná doba je čas medzi nahlásením incidentu verejným obstarávateľom (vrátane užívateľov IS, ktorí nie sú v pracovnoprávnom vzťahu s verejným obstarávateľom) na helpdesk úrovne L3 a jeho prevzatím na riešenie.
- (2) DKVI znamená obnovenie štandardnej prevádzky – čas medzi nahlásením incidentu verejným obstarávateľom a vyriešením incidentu
- úspešným uchádzačom (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť verejného obstarávateľa, ak je potrebná pre vyriešenie incidentu. V prípade potreby je úspešný uchádzač oprávnený požadovať od verejného obstarávateľa schválenie riešenia incidentu.
- (3) Maximálny počet incidentov za kalendárny mesiac. Každá ďalšia chyba nad stanovený limit spoľahlivosti sa počíta ako začatý deň omeškania bez odstránenia vady alebo incidentu. Duplicitné alebo technicky súvisiace incidenty (zadané v rámci jedného pracovného dňa, počas pracovného času 8 hodín) sú považované ako jeden incident.

Incidenty nahlásené verejným obstarávateľom úspešnému uchádzačovi v rámci testovacieho prostredia

1. Majú závažnosť incidentu nekritickú a nižšiu
2. Vzťahujú sa výhradne k dostupnosti testovacieho prostredia
3. Za incident na testovacom prostredí sa nepovažuje incident vztiahnutý k práve testovanej funkcionalite

Vyššie uvedené SLA parametre nebudú použité pre nasledovné služby:

- Služby systémovej podpory na požiadanie (nad paušál)
- Služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien (nad paušál)

Pre tieto služby budú dohodnuté osobitné parametre dodávky.

Časové pokrytie poskytovania služieb

Popis	Parameter	Poznámka
Prevádzkové hodiny	23 hodín	od 1:00 hod. – do 24:00 hod.
Servisné okno	1 hodina	od 0:00 hod. – do 1:00 hod.
Dostupnosť produkčného prostredia IS	98%	· 98% z 24/7/365 t.j. max ročný výpadok je 175 hod. · Maximálny mesačný výpadok je 15 hodín. · Nedostupnosť IS sa počíta od nahlásenia incidentu Zákazníkom. Do dostupnosti IS nie sú započítavané servisné okná a plánované odstávky IS. V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu

8. POŽIADAVKY NA PERSONÁL

Požiadavky na personál boli definované v projektovom zámere v kapitole 8 Projektový tím.

9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Projekt bude v zmysle Vyhlášky 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy realizovaný metódou waterfall.

V zmysle vyhlášky 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy je možné pristupovať k realizácii projektu prostredníctvom čiastkových plnení, t.j. inkrementov. V projekte je definovaný jeden inkrement na obdobie hlavných aktivít.

10. PRÍLOHY