MMB2017000001096

56

Rada města Brna

Z7/31. zasedání Zastupitelstva města Brna
konané dne 5. září 2017

ZM7/2852

Název:
Projekt „Zvýšení odolnosti informační infrastruktury města Brna" – změna parametrů posouzení projektu

Obsah:

- Důvodová zpráva
- Posouzení projektu „Zvýšení odolnosti informační infrastruktury města Brna"
- Návrh architektury kybernetické bezpečnosti (k nahlédnutí)

Návrh usnesení:

Zastupitelstvo města Brna

s c h v a l u j e
aktualizované posouzení projektu „Zvýšení odolnosti informační infrastruktury města Brna" se změnou parametrů, které tvoří přílohu č.... tohoto usnesení

Stanoviska dotčených orgánů:
Materiál byl předložen Radě města Brna na schůzi č. R7/130 konané dne 29. 8. 2017.

Zpracoval:
Odbor implementace evropských fondů
Odbor městské informatiky

Předkládá:
Rada města Brna

Důvodová zpráva

V souladu s čl. 3.1.2. Metodiky implementace projektů (spolu)financovatelných z evropských fondů a národních programům je kolektivním orgánům města Brna předložena **změna parametrů posouzení projektu s názvem „Zvýšení odolnosti informační infrastruktury města Brna"**. Na Z7/029. zasedání Zastupitelstva města Brna konaném dne 20. června 2017 bylo schváleno posouzení projektu a příprava žádosti o dotaci pro tento projekt.

Cílem projektu je vybudovat **Centrum ochrany proti kybernetickým útokům (SOC) pro statutární město Brno a všechny zapojené subjekty**. Metropolitní síť města Brna je opatřením obecné povahy vydaným Národním bezpečnostním úřadem prohlášena za prvek kritické informační infrastruktury státu (dále „KII"), proto je MMB jako její provozovatel povinen zajistit splnění všech požadavků uložených platnou legislativou. Technickým řešením tohoto úkolu je pořízení a implementace komplexních technologií pro vybudování managementu bezpečnostních informací a událostí – Security Information and Event Management. Součástí budou technologie pro monitoring provozních stavů, LOG management a ukládání a vyhodnocování výstupů z KII a souvisejících prvků ICT města a zúčastněných subjektů. Řešení bude splňovat požadované parametry v oblasti důvěrnosti, dostupnosti, citlivosti, autentizace, autorizace, nepopiratelnosti atd.

Dalším důležitým cílem, který bude navýšením rozpočtu projektu realizován, je splnění významné části požadavků nařízení Evropské unie GDPR (General Data Protection Regulation, Obecné nařízení o ochraně osobních údajů).

Podmínky předmětné výzvy umožnují do výstupů projektu zapojit zřizované a zakládané společnosti statutárního města Brna. Do systému bude zapojen MMB, všechny městské části, Městská policie Brno, akciové společnosti s majetkovou účastí města Brna a městem zřizované nemocnice. V prostředí ČR by se mělo jednat o ojedinělý projekt, který zastřeší kybernetickou bezpečnost statutárního města Brna.

Změna parametrů posouzení projektu spočívá ve výrazném rozšíření aktivit a opatření v rámci realizace projektu a navýšení celkových nákladů projektu z 52 520 tis. Kč na 162 000 tis. Kč. Veškeré nové aktivity a opatření jsou způsobilými výdaji projektu a většinu těchto by bylo nutné implementovat i v případě, kdy by se předkládaný projekt nerealizoval, a to vzhledem k nutnosti splnění (nových) legislativních požadavků na bezpečnost informačních systémů města.

V rámci zpracování architektonického konceptu projektu proběhly konzultace se zástupci městských částí statutárního města Brna, se zřizovanými a zakládanými organizacemi statutárního města Brna a s Národním úřadem pro kybernetickou a informační bezpečnost (dále „NÚKIB") s cílem přesně specifikovat a vymezit primární aktivum, které bude předmětem ochrany a soubor opatření, které bude nutno k zajištění ochrany tohoto přijmout. Z uvedené konzultace vyplynuly zvýšené požadavky na rozsah projektu. Dalším vlivem, v důsledku kterého dochází k navýšení rozpočtu projektu, je zákon 205/2017 Sb., o kybernetické bezpečnosti (dále „ZoKB"), který vstoupil v účinnost dne 1. 8. 2017. Zástupci NÚKIB předpokládají, že bude dle ZoKB identifikováno 6 městských akciových společností jako povinný subjekt, na které se zákon bude vztahovat v plném rozsahu.

Definování provedených změn\rozšíření projektu
Skutečný rozsah projektu byl v současnosti definován v materiálu „Návrh architektury kybernetické bezpečnosti", který je pro potřeby kolektivních orgánů dán k nahlédnutí. Tento materiál navrhuje soubor opatření ve struktuře požadované Odborem hlavního architekta MV ČR, který bude návrh architektury a studii proveditelnosti posuzovat a jehož souhlasné stanovisko je podmínkou pro podání žádosti o dotaci.

1. **Navýšení opatření pro komplexní pokrytí požadavků ZoKB u veškerých zapojených společností** a rozšíření z původních 5 na 11 – po detailním průzkumu na základě konzultací na NCKB (dnes NÚKIB) a CRR. Při přípravě původního návrhu jsme vycházeli jen ze splnění základních požadavků ZoKB pomocí návrhu opatření. Byly zde technické kompromisy, další získáné informace ale ukázaly na možnost širšího záběru možných protiopatření a doplnění celého komplexu technologií na typově podobné společnosti.
2. **V úvodních úvahách nebyly zahrnuty všechny technologické prvky a opatření pro BVaK, Úrazovou nemocnici a Nemocnici Milosrdných bratří**, kde nebylo zcela jasné zdali se podle vyhlášky 316/2014 Sb. o kybernetické bezpečnosti na tyto organizace bude ZoKB vztahovat v plné šíři (vyhláška se nyní novelizuje).
3. **Navýšení navrhovaných opatření pro pokrytí požadavků z 8 na 9** (doplněny HoneyPots) – zde jde o doplnění technologických opatření a rozšíření o prvky, které je možno využít k aktivnímu odvracení kyberútoků.
4. **Technicky je vhodné realizovat všechny prvky technologie na typově obdobné společnosti v plné šíři** – což při zvýšení počátečních nákladů (které ale kompenzuje dotace) zajistí do budoucna pokrytí požadavků na protiopatření, vyplývajících ze ZoKB.
5. Vzhledem k pokrytí nákladů dotací z IROP na zvýšení redundance KII zaokruhováním metropolitní sítě se sníží náklady města vyčleněné na tuto akci. **Náklady na zaokruhování** jsou uznatelným výdajem pro IROP (dle výsledků konzultace na CRR).
6. **Systém je navržen jako otevřený, protože se očekává nárůst počtu povinných subjektů pole ZoKB v rámci statutárního města Brna.** Těmto nově určeným organizacím bude dána možnost využití budovaného SOC pro pokrytí požadavků na zajištění vlastní kybernetické bezpečnosti.

Rozsah a synergie projektu byly rovněž konzultovány se zprostředkujícím subjektem poskytovatele dotace Centrem pro regionální rozvoje České republiky (CRR) s doporučením využít v plném rozsahu metodiku stanovení nákladů projektu dle dokumentu IROP.

Předpokládané celkové rozpočtové náklady projektu jsou **162 000 000 Kč. Dotace** by měla dosáhnout výše **145 800 000 Kč** (90 % způsobilých nákladů), přičemž prozatím **veškeré výdaje projektu jsou řazeny do uznatelných nákladů. Finanční spoluúčast statutárního města Brna** se předpokládá ve výši **16 200 000 Kč** (10 % výdajů projektu).
Náklady projektu byly navýšeny pouze o způsobilé výdaje.

Struktura výdajů projektu „Zvýšení odolnosti informační infrastruktury města Brna" (včetně DPH)		
Celkové výdaje projektu	162 000 000 Kč	100 %
Způsobilé výdaje	162 000 000 Kč	100 %
Nezpůsobilé výdaje	0 Kč	0 %
Celková dotace	145 800 000 Kč	90 %
Kofinancování statutárního města Brna	16 200 000 Kč	10 %

Realizace projektu se předpokládá od 1. 1. 2018 – 22. 11. 2019.

Nositelem projektu v souladu s Metodikou implementace projektů (spolu)financovatelných z evropských fondů a národních programů je **Odbor městské informatiky MMB**.

Materiál „Návrh architektury kybernetické bezpečnosti" bude v jednom výtisku předložen k nahlédnutí během zasedání Zastupitelstva města Brna č. Z7/31 dne 5. 9. 2017. Dokument bude rovněž poskytnut předsedům klubů zastupitelů politických stran na CD nosiči.

Stanoviska dotčených orgánů:
Materiál byl předložen Radě města Brna na schůzi č. R7/130 konané dne 29. 8. 2017.
Finanční výbor projednal materiál dne 29. 8. 2017.
Komise Informatiky RMB projedná materiál *per rollam* dne 25.8.2017
Výbor implementace projektů EU projedná materiál *per rollam* dne 25. 8. 2017

bude přílohou unesení

Posouzení projektu *se skládá z těchto částí:*

1. ***Záměr projektu***
   a) Obecné údaje
   b) Legislativní a strategický průmět, popis projektu
   c) Financování
2. ***Analýza dotačních příležitostí***

PROJEKTOVÝ ZÁMĚR – část A.
A.1. PŘEDKLADATEL
1. Plný název předkladatele projektu: Statutární město Brno, Dominikánské náměstí 1, 601 67 Brno
2. Právní statut: Statutární město (dle zákona č. 128/2000 Sb., o obcích)
A.2. KONTAKTNÍ OSOBA A PARTNEŘI PROJEKTU
1. Nositel projektu: Magistrát města Brna, Odbor městské informatiky
2. Jméno kontaktní osoby (nositele): Ing. Jaromír Emmer, vedoucí odboru informatiky
3. Adresa, telefon, mobil, e-mail, webová stránka kontaktní osoby: Ing. Jaromír Emmer Vedoucí OMI MMB emmer.jaromir@brno.cz tel.: 541 173 340
4. Přehled partnerů participujících na projektu:
5. Adresa, telefon, mobil, e-mail, webová stránka dalších partnerů projektu:
6. Způsob spolupráce partnerů na projektu:
A. 3. VŠEOBECNÉ INFORMACE O PROJEKTU
1. Název projektu: Zvýšení odolnosti informační infrastruktury města Brna
2. Umístění projektu: Území statutárního města Brna, budovy Magistrátu města Brna a úřadů městských částí, městské policie Brno, akciové společnosti s majetkovou účastí města Brna, nemocnice zřizované městem Brnem

3. Cíle projektu, jeho účel:

Cílem projektu je vybudování centra ochrany proti kybernetickým útokům pro všechny zúčastněné subjekty v rámci statutárního města Brna – Security Operatipon Centre (dále jen „SOC). Úkolem SOC bude pokrývat procesy potřebné k zajištění provozu, dostupnosti, důvěryhodnosti a integrity služeb informační infrastruktury městských organizací v souladu s požadavky zákona č. 181/2014 Sb. zákona o kybernetické bezpečnosti. Dále bude SOC svými funkcemi tzv. „Log Managementu" a monitoringu pokrývat značnou část požadavků na funkce podle obecného nařízení EU o ochraně osobních údajů (angl. General Data Protection Regulation) neboli GDPR. Cílem je pořídit potřebné komponenty pro pokrytí uvedených činností a implementovat potřebné prvky do funkčního celku.
Agregované výstupy SIEM budou předávány CSIRT (expertní tým pro reakci na počítačové hrozby). Služba CSIRT týmu bude nakupována v rámci provozu SOC. V současnosti je na trhu práce v České republice velice omezené množství kvalifikovaných odborníků a není možné potřebné služby zajistit vlastními zaměstnanci OMI MMB, nebo tyto experty zaměstnat v rámci MMB..

Hlavní komponenty a prvky centra ochrany proti kybernetickým útokům:

- **Security Information and Event Management** (Management bezpečnostních informací a událostí, SIEM). *Jedná se o systém, který svými dotazy získává, analyzuje a koreluje data o událostech v síti. Kombinuje metody detekce a analýzy abnormálních událostí v síti, poskytuje informace nezbytné pro řízení a provádění servisních zákroků.*
  Bude implementován jako technologický celek pro monitoring a management záznamů z ICT komponent, které tvoří struktury informačních systémů u jednotlivých organizací. Cílem je vytvořit technologii v dostatečně robustním provedení pro zabezpečení ochrany získaným provozních informací z rozmanitých ICT prostředí všech zúčastněných subjektů. Řešení musí splňovat požadované parametry v oblasti důvěrnosti, dostupnosti, citlivosti, autentizace, autorizace, nepopiratelnosti. Bude navrhováno jako škálovatelné s možností výkonového a kapacitního růstu včetně dodržení principů architektonické otevřenosti a integrovatelnosti s okolními prvky ICT.
- **Log Management** . *Jedná se o systém, který řídí sběr a uchovávání záznamů o událostech v síti (logů), např. přihlášení a odhlášení uživatelů, kroky provedené administrátory* v rozsahu pokrývajícím HW, SW a licenční potřeby všech zúčastněných subjektů v režimu datově oddělených skladů logů pro dedikované lokality (subjekty). Tato funkcionalita bude zajištěna prvky, které budou zpracovávat vstupní údaje z monitoringu jak pomocí flow sond, tak přímo napojených monitorovacích nástrojů z ICT prvků pokrývané infrastruktury. Získané informace budou využívány rovněž pro potřeby GDPR.
- **Flow Monitoring.** *Systém provádí dlouhodobé detailní monitorování dění (provozu) na počítačové síti. Získané informace o dění na síti a chování uživatelů musí umožnit v reálném čase sledovat a vyhodnocovat bezpečnostní hrozby.* Uplatňuje pokročilé prvky HW a SW řešení pro sledování datových toků s možností vyhodnocování a upozornění na potenciální hrozby při provozu sítí. V rámci sledování datových toků bude také aplikováno vyhodnocování režimů s cílem aktivně reagovat na možná narušení provozu.

4. Výchozí stav:

Současný stav zabezpečení informační infrastruktury subjektů dotčených projektem je řešen individuálně prostřednictvím nástrojů typu firewall, antivirové a antispamové programy. Některé subjekty jsou držiteli certifikátu podle normy ISO IEC 27 001 (TSB, OMI MMB, MpB). Žádné z těchto opatření nesplňuje v plném rozsahu požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti, vyhlášky 316/2017 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) a nařízení GDPR.

Metropolitní síť města Brna je opatřením obecné povahy, vydaném Národním úřadem pro kybernetickou bezpečnost, prohlášena za prvek kritické informační infrastruktury (dále KII), proto je MMB jako její provozovatel povinen zajistit splnění všech požadavků uložených uvedenou legislativou. Provozování KII umožňuje statutárnímu městu Brnu, v rámci parametrů výzvy 10, financování opatření realizovaných MMB a městskými částmi a rovněž opatření realizovaná společnostmi zakládanými a zřizovanými statutárním městem Brnem.
Naplnit na příslušné technické a personální úrovni veškeré požadavky legislativy je pro všechny dotčené subjekty samostatně velmi obtížné a nákladné. **Předkládaný projekt cílí na vybudování jednoho společného centra, ve kterém by byla soustředěna potřebná technologie a SW nástroje k monitoringu a vyhodnocování včetně protiopatření při ochraně infrastruktury všech organizací zapojených do projektu.**

5. Předpokládané výsledky projektu:
Realizací projektu bude docíleno zejména:

- Vybudování technologického centra vybaveného dostatečně robustní technologií a dostatečným počtem licencí SW potřebných k ochraně informačních infrastruktur subjektů zapojených do projektu
- Ochrana všech zúčastněných subjektů proti kybernetickým hrozbám na úrovni odpovídající legislativním požadavkům
- Možnost nastavení jednotné bezpečnostní politiky v rámci statutárního města Brna
- Koordinace vybraných činností vyžadovaných v rámci GDPR
- Vybudování kompetenčního centra
- Většině zapojených subjektů bude poskytnuta ochrana proti kyberútokům na úrovni, které by samostatně nedocílily, z toho plyne též omezení duplicitních nákladů na budování potřebné infrastruktury pro zajištění kyberbezpečnosti;

6. Předpokládané dopady projektu:

- Formulování a schválení memoranda (nebo obdobného dokumentu), kterým se zúčastněné subjekty dobrovolně zaváží k dodržování dohodnutých pravidel v oblasti kyberbezpečnosti a splnění požadavků z dopadů GDPR
- Delegování příslušných pravomocí na provozovatele centra v případě nutnosti rychlého zákroku vyvolaného kyberútokem

7. Cílové skupiny:

- Magistrát města Brna a29 úřadů městských částí
- Městská policie Brno; Brněnské komunikace, a.s.; Dopravní podnik města Brna, a.s.; Lesy města Brna, a.s.; Pohřební a hřbitovní služby města Brna, a.s.; SAKO Brno, a.s.; Starez – sport, a.s.
- Technické sítě Brno, a.s.; Teplárny Brno, a.s.; Veletrhy Brno, a.s.; Brněnské vodárny a kanalizace, a.s
- Nemocnice Milosrdných bratří, příspěvková organizace; Úrazová nemocnice v Brně

PROJEKTOVÝ ZÁMĚR – část B.

B. 1. POPIS PROJEKTU

1. Jednotlivé aktivity projektu:

Předprojektová příprava:

- Návrh bezpečnostní architektury s využitím metodiky TOGAFF
- Zpracování studie proveditelnosti – podrobné zmapování současného stavu a podrobná definice cílů projektu a harmonogramu jejich realizace;
- Zpracování žádosti o dotaci a předložení žádosti o dotaci poskytovateli dotace v systému ISKP

Fyzická realizace projektu:

- Výběrové řízení na dodavatele systému
- Dodávka HW a systémového SW
- Zajištění konektivity všech zapojených subjektů
- Implementace aplikačního SW
- Testování dodaných funkcionalit, import dat, zkušební provoz

Přehled a četnost technických opatření doporučených NUKIB

Technická opatření kybernetické bezpečnosti (rozsah pro studii proveditelnosti 2017)	§16	§17	§18	§19	§21	§22	§23	§24	Počet opatření pro kalkulaci nákladů	
Zajištění monitorování fyzických přístupů k prvkům MSB Monitorování provozních parametrů prostředí u prvků MSB (teplota, ...)	X								1	Sdílené opatření celé SMB
Systém analýzy síťové komunikace (NeFlow, NBA)		X				X			13	Podle počtu subjektů
Systémy pro řízení privilegovaných účtů (PIM / PAM)				X	X				1	Sdílené opatření celé SMB
Logmanagement Systém					X				1	Sdílené opatření celé SMB
Řešení konfiguračního (CMDB) a změnového managementu					X				1	Sdílené opatření celé SMB
Řešení provozního monitoringu						X			1	Sdílené opatření celé SMB
Security Information and Event Management (SIEM) včetně SOC							X		1	Sdílené opatření celé SMB
Automatizované testování zranitelností (Vulnerability testing system)								X	1	Sdílené opatření celé SMB
Honey Poty		X							1	Sdílené opatření celé SMB
Zakruhování Metropolitní sítě Brno	X								1	Sdílené opatření celé SMB

Paragrafy dle vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
§16 Fyzická bezpečnost
§17 Nástroj pro ochranu integrity komunikačních sítí
§18 Nástroj pro ověřování identity uživatelů

§19 Nástroj pro řízení přístupových oprávnění
§20 Nástroj pro ochranu před škodlivým kódem
§21 Nástroj pro zaznamenávání činností
§22 Nástroj pro detekci kybernetických bezpečnostních událostí
§23 Nástroj pro sběr a vyhodnocení kyber. bezpečnostních událostí
§24 Aplikační bezpečnost
§25 Kryptografické prostředky
§26 Nástroje pro zajištění vysoké úrovně dostupnosti

Udržitelnost projektu:

- Zajištění technické a provozní podpory po dobu udržitelnosti projektu
- Akceptace, předání systému do rutinního provozu
- Rutinní provoz systému

2. Časová náročnost projektu:

Předprojektová příprava:

- Návrh bezpečnostní architektury 7/2017
- Zpracování studie proveditelnosti – podrobné zmapování současného stavu a podrobná definice cílů projektu a harmonogramu jejich realizace 7-9/2017
- Vydání souhlasného stanoviska Úřadu vlády a zpracování žádosti o dotaci (8-11/2017)

Fyzická realizace projektu:

- Výběr dodavatele, výběrové řízení, zajištění smluvního vztahu 1/2018-6/2018
- Dodávka HW a systémového SW 6-10/2018
- Zajištění konektivity všech zapojených subjektů 10/2018-2/2019
- Implementace aplikačního SW 2-7/2019
- Testování dodaných funkcionalit, import dat, zkušební provoz a vyhodnocení projektu – nejpozději do 22.11.2019
- zajištění technické a provozní podpory po dobu udržitelnosti projektu – nejpozději do 22.11.2019
- akceptace, předání systému do rutinního provozu – nejpozději do 22.11.2019
- rutinní provoz systému – nejpozději do 22.11.2019

Udržitelnost projektu:
Po dobu pěti let od ukončení realizace projektu.
Harmonogram realizace projektu je předběžně nastaven na 1. 1. 2018 – 22. 11. 2019.
Nejzazší datum pro ukončení projektu je dle pravidel výzvy nastaveno na 22. 11. 2019.

3. Indikátory:
3.04.00 Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti - 1
Zbývající indikátory není možné v současné době specifikovat, jelikož budou výstupem odborně zpracované studie proveditelnosti a finálního nastavení architektury systému.

4. Hrubý rozpočet na celou dobu trvání projektu: (částky uvedené včetně DPH)

Předprojektová příprava	**Původní rozpočet**	**Navýšení rozpočtu**
Studie proveditelnosti	2 000 000 Kč	2 000 000 Kč
Architektura systému	200 000 Kč	200 000 Kč
Realizační fáze projektu		
Administrace VŘ	200 0000 Kč	380 000 Kč
Nákup HW	7 700 000 Kč	25 800 000 Kč
Licence SW	26 400 000 Kč	90 600 000 Kč
Implementace	6 000 000 Kč	21 000 000 Kč
Fyzické zabezpečení	10 000 000 Kč	22 000 000 Kč
Publicita	20 000 Kč	20 000 Kč
Celkem realizace	**52 520 000 Kč**	**162 000 000 Kč**

Náklady na provoz investice po dobu udržitelnosti projektu (5 let) jsou v současnosti odhadovány na 12 640 tis. Kč\rok; celkově tedy 63 200 tis. Kč. Provozní náklady jsou složeny z výdajů na Maintenance licencí 10 240 tis. Kč\rok a náklady na servisní podporu 2 400 tis. Kč\rok.
Náklady jsou vyčísleny na provoz systému pro veškeré zapojené subjekty uvedené v bodě 7 posouzení. Navýšením rozpočtu projektu nedochází k navýšení odhadovaných provozních nákladů systému.

Náklady na servisní podporu zahrnují vysoce expertní služby z oboru kyberbezpečnosti, kdy je zapotřebí disponovat odborníky, kteří jsou schopni vyhodnocovat, analyzovat a aplikovat získané záznamy o událostech (expertní tým pro reakci na počítačové hrozby – CSIRT). V současnosti je na trhu práce v České republice velice omezené množství kvalifikovaných odborníků a není možné potřebné služby zajistit vlastními zaměstnanci OMI MMB, nebo tyto experty zaměstnat v rámci MMB.

Náklady na realizaci a následný provoz projektu budou financovány z rozpočtu statutárního města Brna jako vlastníka a „provozovatele" investice. Metoda a způsob následného rozúčtování nákladů na provoz mezi jednotlivé zapojené subjekty (město, akciové společnosti, příspěvkové organizace) bude řešeno ve studii proveditelnosti. Náklady spojené s udržitelností projektu není možné kofinancovat z IROP ani jiného operačního programu.

B. 2. Strategický a legislativní průmět

1. Soulad se Strategií pro Brno:
Projekt je v souladu se strategií pro Brno, s její částí budování ICT SMB a je v souladu se schválenou Informační strategií.

2. Soulad s odvětvovými koncepčními dokumenty MMB:
Projekt vychází z cílů Informační strategie MMB a je v souladu s architektonickou koncepcí pro oblast ICT řešení v rámci MMB a SMB.

3. Soulad s územním plánem města Brna:
Nerelevantní.

4. Legislativní audit:
Realizace projektu naplní legislativní požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti, vyhlášky 316/2017 Sb. o kybernetické bezpečnosti, nařízení Evropské unie GDPR a požadavky rodiny norem ISO IEC 27 000.

PROJEKTOVÝ ZÁMĚR – část C.

C. 1. FINANCOVÁNÍ

1. Rozpočet na celou dobu trvání projektu:

fáze v Kč	Výdaje na projekt		Příjmy z projektu
	investiční	provozní	
Přípravná Realizační	3 000 000 159 000 000		
Celkem	**162 000 000**		

Náklady na provoz investice po dobu udržitelnosti projektu (5 let) jsou v současnosti odhadovány na 12 640 tis. Kč\rok; celkově tedy 63 200 tis. Kč. Provozní náklady jsou složeny z výdajů na Maintenance licencí 10 240 tis. Kč\rok a náklady na servisní podporu 2 400 tis. Kč\rok.
Náklady jsou vyčísleny na provoz systému pro veškeré zapojené subjekty uvedené v bodě 7 posouzení. Navýšením rozpočtu projektu nedochází k navýšení odhadovaných provozních nákladů systému.

Náklady na servisní podporu zahrnují vysoce expertní služby z oboru kyberbezpečnosti, kdy je zapotřebí disponovat odborníky, kteří jsou schopni vyhodnocovat, analyzovat a aplikovat získané záznamy o událostech (expertní tým pro reakci na počítačové hrozby – CSIRT). V současnosti je na trhu práce v České republice velice omezené množství kvalifikovaných odborníků a není možné potřebné služby zajistit vlastními zaměstnanci OMI MMB, nebo tyto experty zaměstnat v rámci MMB.

Náklady na realizaci a následný provoz projektu budou financovány z rozpočtu statutárního města Brna jako vlastníka a „provozovatele" investice. Metoda a způsob následného rozúčtování nákladů na provoz mezi jednotlivé zapojené subjekty (město, akciové společnosti, příspěvkové organizace) bude řešeno ve studii proveditelnosti. Náklady spojené s udržitelností projektu není možné kofinancovat z IROP ani jiného operačního programu.

2. Možnosti financování

v Kč	Částka	%	Upřesnění
Vlastní zdroje Rozpočet města	16 200 000	10	Fond kofinancování projektů
Ostatní veřejné zdroje EU	145 800 000	90	Integrovaný regionální operační program
Privátní zdroje Jiné			
Celkem	**162 000 000**	**100**	

Náklady na realizaci a následný provoz projektu budou financovány z rozpočtu statutárního města Brna jako vlastníka a „provozovatele" investice. Metoda a způsob následného rozúčtování nákladů na provoz mezi jednotlivé zapojené subjekty (město, akciové společnosti, příspěvkové organizace) bude řešeno ve studii proveditelnosti. Náklady spojené s udržitelností projektu není možné kofinancovat z IROP ani jiného operačního programu.

C. 2. OSTATNÍ INFORMACE
1. Majetkové poměry: Nerelevantní.
2. Synergie: **Zákon o kybernetické bezpečnosti dopadá bez výjimky na MMB, městské části a Městskou polici Brno. Po novele je velmi pravděpodobné, že se bude vztahovat i na většinu městských společností a na vybrané příspěvkové organizace.** Ochranu proti kyberútokům by měla řešit každá organizace ve vlastním zájmu bez ohledu na to, zda je nebo není pod účinností zákona. Z tohoto důvodu je navrhované řešení účinné a nejlevnější a poskytne kvalitní a sofistikovanou ochranu organizacím, které by samostatně tuto problematiku neuměly vyřešit. Vybudované SOC bude zaznamenávat přístupové logy k jednotlivým prvkům sítě, což je jeden z požadavků nařízení GDPR.
3. Zajištění udržitelnosti projektu: Projekt zakládá povinnost udržitelnosti po dobu 5 let. Náklady na realizaci a následný provoz projektu budou financovány pouze z rozpočtu statutárního města Brna jako vlastníka a „provozovatele" investice. Náklady spojené s udržitelností projektu není možné kofinancovat z IROP ani jiného operačního programu.

Analýza dotačních příležitostí

Projekt svojí náplní spadá do „Integrovaného regionálního operačního programu", specifického cíle 3.2 – Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT.

Dle nastavení výzvy je výše podpory pro obce nastavena na 90 % způsobilých výdajů. V rámci IROP jsou nastaveny limity pro hlavní a vedlejší výdaje projektu (struktura stanovena výzvou). Projekt tyto limity s vysokou rezervou splňuje.

Projekt nepřekračuje ani po navýšení rozpočtu maximální výše způsobilých výdajů projektu. Kalkulace projektu je nastavena dle podmínek výzvy jako součet způsobilých opatření (tj. horní hranice způsobilých výdajů projektu) dle jejich specifikace a finančního ohodnocení v textu výzvy.

Rozpočet projektu

Celkové náklady **162 000 000 Kč**
Celkové způsobilé výdaje **162 000 000 Kč**

Rozpočet projektu byl navýšen pouze o způsobilé výdaje.

Zdroje krytí projektu

Financování projektu bude probíhat ve formě ex-post proplacení dotace a je tedy nutné zajištění předfinancování z Fondu kofinancování projektů.

Délka realizace projektu je odhadována na 23 měsíců.

Náklady na realizaci a následný provoz projektu budou financovány z rozpočtu statutárního města Brna jako vlastníka a „provozovatele" investice. Metoda a způsob následného rozúčtování nákladů na provoz mezi jednotlivé zapojené subjekty (město, akciové společnosti, příspěvkové organizace) bude řešeno ve studii proveditelnosti. Náklady spojené s udržitelností projektu není možné kofinancovat z IROP ani jiného operačního programu.

Struktura nákladů projektu

	Původní	Aktuální	%
Předpokládané celkové náklady	**52 520 000 Kč**	**162 000 000 Kč**	**100 %**
Integrovaný regionální operační program	47 268 000 Kč	145 800 000 Kč	90 %
Rozpočet města	5 252 000 Kč	16 200 000 Kč	10 %