MMB2017000000835

61

Rada města Brna

Z7/29. zasedání Zastupitelstva města Brna
konaná dne 20. června 2017

ZM7/2688

Název:
Projekt „Zvýšení odolnosti informační infrastruktury města Brna" - posouzení projektu

Obsah:

- Důvodová zpráva
- Posouzení projektu „Zvýšení odolnosti informační infrastruktury města Brna"

Návrh usnesení:

Zastupitelstvo města Brna

s c h v a l u j e
posouzení projektu „Zvýšení odolnosti informační infrastruktury města Brna", které tvoří přílohu č. … těchto usnesení

s o u h l a s í
s přípravou žádosti o dotaci z Integrovaného regionálního operačního programu na projekt „Zvýšení odolnosti informační infrastruktury města Brna" v rámci parametrů uvedených v posouzení projektu

u k l á d á
Radě města Brna zajistit přípravu žádosti o dotaci z Integrovaného regionálního operačního programu na projekt „Zvýšení odolnosti informační infrastruktury města Brna" v rámci parametrů uvedených v posouzení projektu.

T: 22. 11. 2017

Stanoviska dotčených orgánů:
Materiál byl předložen Radě města Brna na její schůzi č. R7/120 konané dne 13. 6. 2017

Zpracoval:
Odbor implementace evropských fondů
Kancelář náměstka primátora pro oblast Smart city

Předkládá:
Rada města Brna

Důvodová zpráva

V souladu s Metodikou implementace projektů (spolu)financovatelných z evropských fondů a národních programů je voleným orgánům města Brna předloženo posouzení projektu s názvem „Zvýšení odolnosti informační infrastruktury města Brna".

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

Cílem projektu je vybudovat **Centrum ochrany proti kybernetickým útokům 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, proto je MMB jako její provozovatel povinen zajistit splnění všech požadavků uložených platnou legislativou. Technickým řešením tohoto úkolu je vybudování managementu bezpečnostních informací a událostí – Security Information and Event Management. Řešení bude splňovat požadované parametry v oblasti důvěrnosti, dostupnosti, citlivosti, autentizace, autorizace, nepopiratelnosti atd.

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 rámci přípravy projektové záměru byly tyto osloveny s žádostí o poskytnutí informací o IT infrastruktuře, na základě kterých byl proveden odhad rozsahu technologií, počtu licencí a implementace systému. V prostředí ČR by se mělo jednat o ojedinělý projekt, který zastřeší kybernetickou bezpečnost statutárního města Brna.

Předpokládané celkové rozpočtové náklady jsou **40 820 tis. Kč**. **Dotace** by měla dosáhnout výše **36 738 tis. Kč** (90 % způsobilých nákladů). Veškeré náklady projektu jsou řazeny mezi způsobilé. **Finanční spoluúčast statutárního města Brna** se předpokládá ve výši **4 082 tis. Kč** (10 % celkových výdajů projektu).

Struktura výdajů projektu „Zvýšení odolnosti informační infrastruktury města Brna" (včetně DPH)		
Celkové výdaje projektu	40 820 000 Kč	100 %
Způsobilé výdaje	40 820 000 Kč	100 %
Celková dotace	36 738 000 Kč	90 %
Kofinancování statutárního města Brna	4 082 000 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 OMI MMB.

Stanoviska dotčených orgánů:
Materiál nebyl z časových důvodů projednán v komisích RMB
Výbor implementace projektů EU projedná materiál dne 9. 6. 2017

bude přílohou usnesení

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.

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 získaných 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 bezpečnostním úřadem, 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
- 29 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

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 7-8/2017
- 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:
V současnosti není možné specifikovat. Bude výstupem odborně zpracování studie proveditelnosti a nastavení architektury systému.

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

Předprojektová příprava	
Studie proveditelnosti	300 000 Kč
Bezpečnostní architektura	200 000 Kč
Realizační fáze projektu	
Administrace VŘ	200 000 Kč
Nákup Hardware	7 700 000 Kč
Nákup licencí Software	26 400 000 Kč
Implementace a nasazení aplikace	6 000 000 Kč
Povinná publicita projektu	20 000 Kč
Celkem realizace	**40 820 000 Kč**

Realizační fáze projektu

Nákup Hardware:
Servery SIEM; Firewall; Kolektor
Virtualizace 6 serverů; Switch
NAS Network Attached Storage

Nákup licencí Software:
SEIM; Windows Terminal Server
VM ware; Sondy a kolektory flow
PAM (Privileg Access Monitoring)

Implementace a nasazení aplikace:
Analytické, implementační práce, školení a metodická podpora;
Provedení preanalýzy, reporting a přístupové role;
Nastavení procesů, přístupových práv a reportů

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 všech 43 zapojených subjektů uvedených v bodě 7 posouzení – cílové subjekty: MMB, 29 ÚMČ, MpB; BKOM; DPMB; Lesy města Brna, a.s.; Pohřební a hřbitovní služby města Brna, a.s.; SAKO Brno; Starez; TSB.; Teplárny Brno, a.s.; BVV; BVaK; Nemocnice Milosrdných bratří, příspěvková organizace; Úrazová nemocnice v Brně.

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. 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 komise 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	500 000		
Realizační	40 320 000		
Celkem	**40 820 000**		

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 všech 43 zapojených subjektů uvedených v bodě 7 posouzení – cílové subjekty: MMB, 29 ÚMČ, MpB; BKOM; DPMB; Lesy města Brna, a.s.; Pohřební a hřbitovní služby města Brna, a.s.; SAKO Brno; Starez; TSB.; Teplárny Brno, a.s.; BVV; BVaK; Nemocnice Milosrdných bratří, příspěvková organizace; Úrazová nemocnice v Brně.

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. 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	4 082 000	10	Fond kofinancování projektů
Ostatní veřejné zdroje			
EU	36 738 000	90	Integrovaný regionální operační program
Privátní zdroje			
Jiné			
Celkem	**40 820 000**	**100**	

Náklady na realizaci a následný provoz projektu budou financovány z rozpočtu statutárního města Brna jako vlastníka a „provozovatele" investice. 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.

Rozpočet projektu na přípravu projektové dokumentace

Celkové náklady **40 820 000 Kč**
Celkové způsobilé výdaje **40 820 000 Kč**

Zdroje krytí projektu

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

Délka realizace projektu je odhadována na 23 měsíců.

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.

Struktura nákladů projektu

Předpokládané celkové náklady	**40 820 000 Kč**	**100 %**
Integrovaný regionální operační program	36 738 000 Kč	90 %
Rozpočet města	4 082 000 Kč	10 %