Z9/02. zasedání Zastupitelstva města Brna
konané dne 15.11.2022

55. Projekt "Rozšíření monitoringu a logování síťových prvků SMB" - posouzení projektu

Anotace

Posouzení projektu "Rozšíření monitoringu a logování síťových prvků SMB" podané v rámci Integrovaného regionálního operačního programu. Cílem projektu je zapojení moderních bezpečnostních technologií, které poskytují dohled, dozor a umožňují detekci, reakci a zpětnou analýzu anomálií v chování počítačových sítí SMB. Celkové způsobilé náklady projektu jsou vyčísleny na částce 5 121 020 Kč. Dle Specifických pravidel výzvy je pro územní samosprávný celek míra poskytované dotace 85 % způsobilých výdajů, což činí 4 352 867 Kč. Spolufinancování ve výši zbývajících 15 % pak činí 768 153 Kč.

Návrh usnesení

Zastupitelstvo města Brna

1. bere na vědomí schválení posouzení projektu "Rozšíření monitoringu a logování síťových prvků SMB" Radou města Brna na základě čl. 3.1.1 Metodiky implementace projektů (spolu)financovatelných z evropských fondů a národních programů, s ohledem na termín pro podání žádosti o dotaci

Stanoviska

Materiál projednala Rada města Brna na R8/238. schůzi konané dne 21.9. a doporučila Zastupitelstvu města Brna přijmout výše uvedený návrh usnesení.

Podpis zpracovatele pro archivaci

Zpracovatel

Elektronicky podepsáno
Ing. Ivan Hloušek
vedoucí odboru - Odbor implementace evropských fondů
8.11.2022 v 09:53
Garance správnosti, zákonnosti materiálu

Spolupodepisovatel

Elektronicky podepsáno
Ing. David Menšík
vedoucí odboru - Odbor městské informatiky
8.11.2022 v 13:01

Spolupodepisovatel

Elektronicky podepsáno
Mgr. Radek Řeřicha
vedoucí Úseku 4. náměstka primátorky - Úsek 4. náměstka primátorky
8.11.2022 v 11:06

Obsah materiálu

Důvodová zpráva

V souladu s Metodikou implementace projektů (spolu)financovatelných z evropských fondů a národních programů je voleným orgánům města předloženo posouzení projektu k projektu s názvem **Rozšíření monitoringu a logování síťových prvků SMB** do Integrovaného regionálního operačního programu (dále také „IROP“).

Předkládaný projekt je řešen ve dvou rovinách – **Log Management** a **Obnova a rozvoj nástrojů FLOWMON**. Obě části projektu se budou realizovat paralelně. Tento systém je nastavený tak, aby monitoroval interní prostředí Metropolitní sítě Statutárního města Brna, s tím, že bude zajištěna odpovídající úroveň soukromí uživatelů a systém bude jen v nezbytně nutné míře monitorovat provoz odcházející do veřejné sítě internetu.

Metropolitní síť, sestávající z více redundantních datových center, bude hlídána robustním **systémem sond typu Flowmon**, z nichž některé mají jako součást své výbavy moduly IDS (tj. systém pro odhalení průniku), a díky bezpečnému kanálu z dozorového centra jsou schopny proaktivního zásahu v režimu 24/7. Všechny klíčové systémy, identifikované v rámci analýzy rizik, budou pod neustálým dohledem, který bude zajišťovat vrstvená síť dozorových sond. Výstupy dozorových sond jsou k dispozici technickému pracovníkovi OMI MMB, který identifikuje provozní výpadky a slabá místa po dobu úředních hodin, případně během obvyklé pracovní doby pracovišť MMB.

Výstupy budou proaktivně automatizovaným řešením předávány do centralizovaného **Log Managementu (dále také „LM“)**, který podporuje základní komponentu typu SIEM (tj. monitoring informací a událostí bezpečnosti). Výstupy ze sond nejvyšší úrovně a výstupy z nástroje SIEM budou k dispozici dozorovému týmu společnosti Technické sítě Brno, a.s. který má, mimo svoji pracovní dobu, pasivní dohledový režim se zasíláním upozornění na kritické události a je schopen urychlit reakci týmu, který se postará o zásah v rámci napadené části sítě.

Díky využívání jednotného LM je také možné vybrané nekritické problémy analyzovat zpětně, ať už z důvodu pozdější nutné spolupráce s Orgány činnými v **trestním** řízení, nebo z důvodu usnadnění či umožnění servisních zásahů pracovníkům OMI MMB či externích dodavatelských společností.
Robustní reaktivní analýza sítě pomocí systému Log Management v kombinaci s víceúrovňovým monitoringem prostřednictvím sond povede ke zvýšené efektivitě a bezpečnosti provozovaných systémů, a díky kontinuálnímu sledování stavu sítě a vykrývání či prevenci možných chyb, nepřímo komfort občanů i pracovníků OMI MMB. Materiál projednal Výbor pro řízení kybernetické bezpečnosti statutárního města Brna dne 14.9.2022 a schválil jej jednomyslně 7 členy.

Předpokládané období realizace: **1. 2. 2023 – 30. 3. 2024 (14 měsíců).**

Projekt byl podán ve výzvě č. **4. Integrovaného regionálního operačního programu – Kybernetická bezpečnost – SC 1.1 (PR),** která byla vyhlášena 16. 8. 2022. Ukončení příjmu žádosti bylo stanoveno k datu 30. 9. 2022.

Celkové způsobilé náklady projektu jsou vyčísleny na částce **5 121 020 Kč.** Dle Specifických pravidel výzvy je pro územní samosprávný celek v přechodovém regionu, jako žadatele, míra poskytované dotace 85 % způsobilých výdajů, což činí **4 352 867 Kč**. Spolufinancování ve výši zbývajících 15 % pak činí **768 153 Kč.**

Struktura výdajů projektu „Rozšíření monitoringu a logování síťových prvků SMB“ (včetně DPH)		
Celkové výdaje projektu	5 121 020 Kč	100 %
Nezpůsobilé výdaje	0 Kč	0 %
Způsobilé výdaje	5 121 020 Kč	**100 %**
Výše dotace	**4 352 867 Kč**	**85 %**
Kofinancování města Brna	**768 153 Kč**	**15 %**

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

Stanoviska dotčených orgánů:

Materiál nepodléhá projednání v komisích RMB.

Rada města Brna projednala materiál na schůzi č. R8/238. konané dne 21. 9. 2022. Schváleno jednomyslně 11 členy.
Hlasování: 11-pro, 0-proti, 0-se zdržel/z 11 členů.

JUDr. Vaňková	Mgr. Hladík	Bc. Koláčný	JUDr. Oliva	JUDr. Kerndl	Róbert Čuma	Ing. Fišer	Ing. Grund	RNDr. Chvátal	Ing. Kratochvíl	Mgr. Suchý
pro	pro	pro	pro	pro	pro	pro	pro	pro	pro	pro

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, 602 00 Brno

2. Právní statut:
statutární město (dle zákona č. 128/2000 Sb., o obcích)

A. 2. KONTAKTNÍ OSOBA A PARTNEŘI PROJEKTU

1. Nositel projektu: Odbor městské informatiky MMB

2. Jméno kontaktní osoby (nositele): Ing. Dušan Hájek; Ing. David Menšík

3. Adresa, telefon, mobil, e-mail, webová stránka kontaktní osoby:
Malinovského nám. 3, 60200 Brno
721 563 501; 602 564 698;
hajek.dusan@brno.cz; mensik.david@brno.cz;

4. Přehled partnerů participujících na projektu:
Projekt nezakládá partnerství.

A. 3. VŠEOBECNÉ INFORMACE O PROJEKTU

1. Název projektu: Rozšíření monitoringu a logování síťových prvků SMB

2. Umístění projektu: Statutární město Brno

3. Cíle projektu, jeho účel:
Zapojení moderních bezpečnostních technologií, které poskytují dohled (dále také „pasivní monitoring“), dozor (dále také „aktivní monitoring“) a umožňují detekci, reakci a zpětnou analýzu anomálií v chování počítačových sítí SMB.

4. Výchozí stav:

Statutární město Brno v současné době provozuje osm významných agendových informačních systémů, které jsou ve správě Odboru městské informatiky Statutárního města Brna (dále také jako „OMI SMB“ a jsou poskytovány centrálně městským částem. Dále má město stanovený rozsah Systému řízení bezpečnosti informací, který obsahuje deset klíčových systémů, které město považuje za nezbytné pro zajištění chodu úřadu i agend. V uživatelské roli využívá větší množství ISVS, prostřednictvím kterých plní svoje povinnosti statutárního města v souladu se Zákonem 128/2000 Sb., o obcích v platném znění. O obsluhu a provoz těchto systémů se stará OMI SMB, na zajištění bezpečnosti se podílí Kancelář kybernetické bezpečnosti Statutárního města Brna a při plnění úkolů asistují také externí smluvní subjekty.
Problematika dozoru nad systémy SMB je řešena víceúrovňově, částečně prostřednictvím pracovníků SMB a jejich dvou sond typu Flowmon od společnosti KEMP, které pokrývají aktivní monitoring v režimu 8/5, tedy osm hodin po dobu pěti dní v týdnu, částečně prostřednictvím dozorového týmu společnosti Technické sítě Brno, a.s. který má dozorové pracoviště, vybavené sondou typu GreyCortex Mendel, které je rovněž v provozu v režimu 8/5 a dále prostřednictvím dohledu v režimu 24/7. Reakční doby mimo pracovní dobu jsou pokryty smluvně, nicméně neexistuje systém včasného varování.
Analýza událostí je závislá na tom, zda lze ze systému, na kterém anomálie vznikla ručně zajistit logy, případně systém celý bezpečným způsobem včas odstavit a získat z něj záznam událostí, který se následně analyzuje.
Proaktivní řešení vznikajících problémů je nad stávající technické i personální možnosti pracovníků města.

5. Předpokládané výsledky projektu:
Metropolitní síť, sestávající z více redundantních datových center, je hlídána robustním systémem sond typu Flowmon, z nichž některé mají jako součást své výbavy moduly IDS a díky bezpečnému kanálu z dozorového centra jsou schopny proaktivního zásahu v režimu 24/7.
Všechny klíčové systémy, identifikované v rámci analýzy rizik a popsané buď v rozsahu SŘBI, nebo podporující agendy v přenesené působnosti města, jsou pod neustálým dohledem, který zajišťuje vrstvená síť dozorových

sond. Výstupy dozorových sond jsou k dispozici technickému pracovníkovi OMI MMB, který identifikuje provozní výpadky a slabá místa po dobu úředních hodin, případně během obvyklé pracovní doby pracovišť MMB.
Rovněž jsou proaktivně automatizovaným řešením předávány do centralizovaného Log Managementu (dále také „LM“), který podporuje základní komponentu typu SIEM. Výstupy ze sond nejvyšší úrovně a výstupy z nástroje SIEM jsou k dispozici dozorovému týmu společnosti Technické sítě Brno, a.s. který má mimo svoji pracovní dobu pasivní dohledový režim se zasíláním upozornění na kritické události a je schopen urychlit reakci týmu který se postará o zásah v rámci napadené části sítě.
Díky využívání jednotného LM je také možné vybrané nekritické problémy analyzovat zpětně ať už z důvodu pozdější nutné spolupráce s Orgány činnými v trestním řízení, nebo z důvodu usnadnění či umožnění servisních zásahů pracovníkům OMI MMB či externích dodavatelských společností.
Robustní reaktivní analýza sítě pomocí systému Log Management v kombinaci s víceúrovňovým monitoringem prostřednictvím sond vede ke zvýšené efektivitě a bezpečnosti provozovaných systémů a díky kontinuálnímu sledování stavu sítě a vykrývání či prevenci možných chyb nepřímo komfort občanů i pracovníků OMI MMB.

6. Předpokládané dopady projektu:
Celý systém je nastavený tak, aby monitoroval primárně interní prostředí Metropolitní sítě Statutárního města Brna, s tím, že bude zajištěna odpovídající úroveň soukromí uživatelů a systém bude jen v nezbytně nutné míře monitorovat provoz odcházející do veřejné sítě internetu.

7. Cílové skupiny:
- Instituce veřejné správy
- Zaměstnanci veřejné správy

Jedná se o uživatele Statutárního města Brno, tzn. uživatele městských částí, a dalších subjektů přistupující k infrastruktuře prostřednictvím Metropolitní sítě.

PROJEKTOVÝ ZÁMĚR – část B.

B. 1. POPIS PROJEKTU

1. Jednotlivé aktivity projektu:

KA – Kybernetická bezpečnost

Do klíčové aktivity spadají všechny integrální součásti projektu a jsou řešeny ve dvou rovinách – **A. Log Management** a **B. Obnova a rozvoj nástrojů FLOWMON**. Obě části projektu jsou chronologicky rozděleny do etap a jejich realizace bude probíhat paralelně.

A. Log Managment:

Fáze 1:

- provedení detailní analýzy procesních, funkčních a technických požadavků na řešení, jejich detailní rozpracování a verifikace s určenými pracovníky za účelem ověření správnosti a vhodnosti navrženého postupu a jeho optimalizace
- zpracování implementační studie a harmonogramu implementace včetně definice klíčových implementačních milníků

Fáze 2:

dodání HW a SW

- vlastní implementace LM a integrace do prostředí MMB
- vytvoření provozní (uživatelské a administrátorské), technické a bezpečnostní dokumentace
- školení pro obsluhu LM v předpokládaném rozsahu max. 5 dnů pro max. 10 osob
- provozní a funkční testování dle odsouhlasené implementační studie a návazné bezpečnostní testování vybraným subjektem
- zajištění přípravy nasazení a vlastní nasazení LM do produkčního provozu
- ověření funkčnosti LM v pilotním (ověřovacím provozu)

Fáze 3:

- poskytování údržby a technické podpory LM (včetně SLA) na dobu 5 let, zahrnující služby maintenance licencí (full maintenance) a podporu provozu LM, aktualizace veškeré uživatelské a technické dokumentace k LM minimálně jedenkrát ročně
- poskytování služeb rozvoje LM na dobu 5 let od akceptace

B. Obnova a rozvoj nástrojů FLOWMON (pro behaviorální analýzu síťového provozu, monitoringu vybraných aplikací a detekci síťového provozu)

Fáze 1:

- Realizační projekt - provedení detailní analýzy procesních, funkčních a technických požadavků na řešení, jejich detailní rozpracování a verifikace s určenými pracovníky za účelem ověření správnosti a vhodnosti navrženého postupu a jeho optimalizace

Fáze 2:

- Dodávku HW appliance – sond a kolektoru potřebných pro provoz systému
- Dodávku virtuální appliance – kolektoru potřebného pro provoz systému
- Dodávku SW pro detekci anomálií
- Dodávku SW pro packet capturing
- Dodávku SW pro monitoring aplikací
- Implementaci HW a SW do prostředí statutárního města Brna

Fáze 3:

- Technická podpora od výrobce ne veškeré požadované komponenty po dobu 60 měsíců
- Trvalý dohled nad bezpečnostními událostmi systému pro detekci anomálií implementovaných zařízení v režimu 24x7 po dobu 60 měsíců
- Technický dohled nad bezpečnostními událostmi systému ADS implementovaných zařízení **v režimu 24x7**
- Řešení vzniklých událostí **v režimu 8x5** ve spolupráci se zadavatelem
- Záznam událostí do ticketovacího systému včetně jednoduché informace o dané události z pohledu bezpečnosti
- Centralizovaný dashboard pro jednoduchý přístup k informacím
- Zajištění bezpečného přístupu do systému přes IPSec tunel

- Report vzniklých událostí na měsíční bázi

2. Časová náročnost projektu:
14 měsíců

Předpokládané období realizace: 1. 2. 2023 – 30. 3. 2024

Fáze 1: 60 dní od podpisu smlouvy
Fáze 2. 200 dní od fáze 1
Fáze 3: 60 měsíců od akceptace

3. Indikátory:

304 002 - Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti - 21

4. Hrubý rozpočet na celou dobu trvání projektu:

Vzhledem k nastavení kategorii způsobilých výdajů dle Specifických pravidel 4. výzvy – Kybernetická bezpečnost (PR), je způsobilá pouze část projektu:

Způsobilé výdaje:

- Přímé náklady

A. Log Managment:

1 406 000 Kč – Pořízení dlouhodobého hmotného majetku – SW a HW
- náklady na HW
- licence SW
- implementace a customizace řešení

B. Obnova a rozvoj nástrojů FLOWMON

3 380 000 Kč – Pořízení dlouhodobého hmotného majetku – SW a HW
- náklady na HW
- licence SW
- implementace a customizace řešení

- Nepřímé náklady

Jedná se o paušální sazbu 7 % z přímých nákladů. Zde budou zahrnuty náklady na realizační projekt Obnova a rozvoj nástrojů FLOWMON, zhotovení implementační studie Log Management, atd.

B. 2. STRATEGICKÝ A LEGISLATIVNÍ PRŮMĚT

1. Soulad se Strategií Brno 2050:
Projekt je v souladu se strategií #brno2050, a to s hodnotou **Efektivní elektronická správa a otevřená data**, s dílčím cílem B „Zabezpečit kontinuitu provozu, zabezpečit data a komunikaci proti ztrátě nebo zneužití (vč. bezpečnostní strategie)“, prioritou B1 „Zajistit kvalitní a bezpečnou datovou infrastrukturu ve vysoké dostupnosti“.

2. Soulad s odvětvovými koncepčními dokumenty MMB:
Projekt svým charakterem přímo spadá do Informační strategie města Brna 2022-2026

3. Soulad s územním plánem města Brna:
Nerelevantní

4. Legislativní audit:
Nerelevantní

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 provozní	5 121 020	0	
Celkem	**5 121 020**	**0**	

Celkový rozpočet alokovaný pro investiční aktivity města Brna je ve výši 5 121 020 Kč a jedná se o způsobilé výdaje projektu. Náklady na provoz jsou vyčísleny na hodnotě 10 647 000 Kč a budou financovány z rozpočtu OMI MMB (mimo projekt).

2. Možnosti financování

v Kč	Částka	%	Upřesnění
Vlastní zdroje Rozpočet města	768 153	15	Fond kofinancování projektů
Ostatní veřejné zdroje EU	4 352 867	85	Integrovaný regionální operační program
Privátní zdroje jiné			
Celkem	**5 121 020**	**100**	

C. 2. OSTATNÍ INFORMACE

1. Majetkové poměry:
Nabyvatelem veškerého majetku, jenž vznikne v rámci realizace projektu, bude statutární město Brno.

2. Synergie:
Projekt nemá aktuálně zajištěnou žádnou synergii s dalšími projekty, avšak svou povahou je synergický s Informační strategii města Brna 2022-2026.

3. Zajištění udržitelnosti projektu:
Udržitelnost projektu bude v souladu se Specifickými pravidly 4. výzvy – Kybernetická bezpečnost. Z rozpočtu města Brna bude zajištěno financování veškerých výdajů spojených s provozem a údržbou pořízených prvků kybernetické bezpečnosti. Rovněž bude zajištěno, aby pořízené prvky kybernetické bezpečnosti sloužily svému účelu.

Analýza dotačních příležitostí

Projekt **„Rozšíření monitoringu a logování síťových prvků SMB“** svým zaměřením v souladu s Integrovaným regionálním operačním programem (IROP), s cílem politiky Konkurenceschopnější a inteligentnější Evropa, s prioritou Zlepšení výkonu veřejné správy a specifickým cílem Využívání přínosů digitalizace pro občany, podniky, výzkumné organizace a veřejné orgány

Projekt bude podán ve výzvě č. **4. výzva IROP - Kybernetická bezpečnost – SC 1.1 (PR),** která byla vyhlášena 16. 8. 2022. Ukončení příjmu žádosti bylo stanoveno k datu 30. 9. 2022.
Celkové způsobilé výdaje na projekt činí **5 121 020 Kč**, podle předběžné analýzy bude způsobilým výdajem pouze investiční část projektu, která je zaměřena na pořízení a implementaci HW a SW. Veškeré provozní náklady na poskytování služeb údržby, podpory, rozvoje a dohledového centra zmíněných nástrojů jsou dle nastavení výzvy nezpůsobilé a budou hrazeny z rozpočtu OMI MMB.

Dle Specifických pravidel výzvy je pro územní samosprávný celek v přechodovém regionu, jako žadatele, míra poskytované dotace 85 % způsobilých výdajů, což činí **4 352 867 K**č. Spolufinancování ve výši zbývajících 15 % pak činí **768 153 Kč.**

Rozpočet projektu
Předpokládaný rozpočet je navržen následovně:

Celkové výdaje projektu	5 121 020 Kč	100 %
Nezpůsobilé výdaje	0 Kč	0 %
Způsobilé výdaje	5 121 020 Kč	100 %
Výše dotace	**4 352 867 Kč**	**85 %**
Kofinancování města Brna	**768 153 Kč**	**15 %**

Zdroje krytí projektu
Dle Specifických pravidel výzvy je pro územní samosprávný celek v přechodovém regionu, jako žadatele, míra poskytované dotace 85 % způsobilých výdajů. Spoluúčast bude hrazena z Fondu kofinancování projektů.
Financování projektu bude probíhat v režimu ex-post. Předfinancování projektu bude zajištěno z rozpočtu města.