Materiál č.

19

A. Materiál:

Bod rokovania	**Schválenie podania žiadosti o nenávratný finančný príspevok – „Zvýšenie úrovne informačnej a kybernetickej bezpečnosti mesta Ružomberok“**
Dátum rokovania MsZ	**28.09. 2022**
Predložené poslancom MsZ	**21.9.2022**
Predkladateľ	Ing. Ján Bednárik, 2. viceprimátor primátor mesta
Spravodajca	Ing. Martin Žabenský, poverený vedením Oddelenia IT
Na základe	Výzvy Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. OPII-2021/7/16-DOP so zameraním na „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“
Stanovisko MsR zo dňa 14.09.2022	**MsR odporúča MsZ schváliť** materiál v predkladanom znení Hlasovanie: 3-0-0
Zoznam príloh	Výzva Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. OPII-2021/7/16-DOP so zameraním na „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“

B. Návrh na uznesenie:
Mestské zastupiteľstvo v Ružomberku:

I. schvaľuje

a) súhlas s podaním žiadosti o nenávratný finančný príspevok s názvom: „Zvýšenie úrovne informačnej a kybernetickej bezpečnosti mesta Ružomberok“ v rámci výzvy OPII-2021/7/16-DOP,

b) súhlas so zabezpečením povinného spolufinancovania projektu v sume 9 837,83 € t.j. min. 5% z celkových oprávnených výdavkov,

c) súhlas so zabezpečením financovania neoprávnených výdavkov, ktoré vzniknú v priebehu realizácie projektu a budú nevyhnutné na dosiahnutie jeho cieľa.

C. Dôvodová správa

Výzva „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“ (ďalej ako „výzva“) umožňuje žiadať o projekty najmä v týchto oblastiach:

- inventarizácia, klasifikácia a kategorizácia informačných aktív, realizácia AR/BIA, riadenie rizík a spracovanie základných dokumentov v oblasti IB a KyB v zmysle zákona č. 69/2018 Z.z.,
- pilotná implementácia systému pre logmanažment, zahŕňajúca predovšetkým práce na zmapovaní zdrojov logov a ich napojení na centrálny log manažment nástroj pre následné nasadenie SIEM riešení,
- pilotná implementácia SOC as a service,
- pilotná implementácia dvojfaktorovej autentifikácie a mobile device managementu.

Podpora bude primárne poskytovaná pre oblasti:

- governance informačnej a kybernetickej bezpečnosti (IB a KyB) a bezpečnostná dokumentácia,
- riadenie aktív, hrozieb a rizík, t.j. inventarizácia aktív, klasifikácia a kategorizácia aktív, spolu s vykonaním analýzy rizík a analýzy dopadov a následným riadením identifikovaných rizík.

Tieto aktivity totiž predstavujú nevyhnutný a nutný základ pre riadenie IB a KyB a pre ďalší rozvoj v tejto oblasti a implementáciu dodatočných bezpečnostných opatrení a technických bezpečnostných riešení. Výstupy týchto aktivít sú nevyhnutným predpokladom pre prijímanie adekvátnych, efektívnych, vyvážených a optimálnych bezpečnostných opatrení.

Podpora pre iné oblasti riadenia IB a KyB bude poskytovaná len pre tie inštitúcie, ktoré preukážu, že tieto oblasti majú plne pokryté a výstupy z týchto aktivít sú k dispozícii pre rozvoj ďalších oblastí riadenia IB a KyB uvedených vyššie. Preukázanie realizácie a naplnenia týchto základných aktivít bude nevyhnutnou podmienkou pre žiadanie finančných prostriedkov na aktivity typu bezpečnostného monitoringu, riadenia bezpečnosti prevádzky, riadenia prístupov a BCM a implementácie ďalších bezpečnostných riešení a funkcii ako sú napr. IAM, DLP, 2FA, VS, LMS, SIEM/SOC a pod.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky bude pre potenciálnych žiadateľov poskytovať najmä:

- šablóny pre dokumenty vyplývajúce zo zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
- usmernenia a odporúčania k prispôsobeniu dokumentov a riadeniu IB a KyB,
- metodiku spracovania AR/BIA a riadenia rizík.

Výsledkom projektu sú inštitúcie zapojené do projektu, ktoré si efektívnym spôsobom implementujú klasifikáciu a kategorizáciu, realizáciu AR/BIA, riadenie rizík a základné dokumenty a rámce riadenia informačnej a kybernetickej bezpečnosti. Zároveň, ak zostanú finančné prostriedky, bude možnosť overiť spôsob implementácie log manažment systému v

prostredí štátnej správy, ako aj životaschopnosť služby SOC as a service v porovnaní s veľkými SOC projektmi, ktoré sú aktuálne v realizácii.

Oprávnenými žiadateľmi môžu byť organizácie štátnej alebo verejnej správy, obce so štatútom mesta a vyššie územné celky. Jednotliví žiadatelia budú zoradení podľa dopadu potenciálneho kybernetického incidentu na daného žiadateľa, resp. spoločnosť. Časová oprávnenosť realizácie aktivít projektu:
- začiatok realizácie aktivít projektu nesmie nastať pred 01.01.2014 pričom aktivity projektu musia byť ukončené najneskôr k 31.12.2023.
Odporúča sa žiadateľom ukončiť fyzickú realizáciu aktivít projektu najneskôr 3 mesiace pred 31.12.2023, za účelom plynulého finančného vysporiadania projektu, t .j . do 31.12.2023.

Maximálna a minimálna výška:
- minimálna výška nenávratného finančného príspevku na projekt sa stanovuje na 70 000 EUR
- maximálna výška nenávratného finančného príspevku na projekt sa stanovuje na 450 000 EUR.

Stručný popis projektu:

Projekt „Zvýšenie úrovne informačnej a kybernetickej bezpečnosti mesta Ružomberok“ sa zameriava na vytvorenie komplexného technického riešenia, ktoré umožní zvýšiť úroveň kybernetickej a informačnej bezpečnosti okresného mesta Ružomberok. Rozsah navrhovaných riešení priamo reflektuje na závery auditu kybernetickej bezpečnosti, ktorý samospráva podstúpila v priebehu roka 2021 a ukončila ho v roku 2022. Projekt bude implementovaný prostredníctvom štyroch hlavných aktivít, ktorými sú:

- Analýza a Dizajn
- Nákup technických prostriedkov, programových prostriedkov a služieb
- Implementácia a Testovanie
- Nasadenie

Hlavné aktivity projektu budú realizované celkovo v rámci piatich modulov, medzi ktoré patria:

- Nasadenie informačného systému pre identifikáciu a riadenie rizík v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§6)
- Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)
- Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti – softvér
- Zriadenie SOC ako služby v prevádzke 24/7
- Nasadenie DLP Realizácia hlavných aktivít projektu v rámci navrhovaných technických celkov (modulov) prispeje k naplneniu hlavného cieľa projektu, ktorým je: „Rozvoj úrovne informačnej a kybernetickej bezpečnosti prostredníctvom zavedenia adekvátnych, efektívnych, vyvážených a optimálnych bezpečnostných opatrení“.

Dôkazom dosiahnutia hlavného cieľa projektu bude naplnenie nasledovných merateľných ukazovateľov:
• P0048 Dodatočný počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov: 3
• P0193 Počet nasadených nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov: 5
• P0167 Počet informačných systémov VS zapojených do centrálneho systému monitorovania bezpečnosti v rámci VS: 3

Rozpočet:
Celková výška oprávnených výdavkov: 196 756,64 €
Percento spolufinancovania zo zdrojov EÚ a ŠR: 95 %
Žiadaná výška nenávratného finančného príspevku: 186 918,81 €
Výška spolufinancovania z vlastných zdrojov: 9 837,83

D. Dopad na rozpočet:

- Zabezpečenie financovania prípadných neoprávnených výdavkov rozpočtu mesta.
- Zabezpečenie finančných prostriedkov na spolufinancovanie realizovaného projektu vo výške rozdielu celkových výdavkov projektu a poskytnutého NFP v súlade s podmienkami pomoci.