Hodnota za peniaze projektu

Kybernetická bezpečnosť v samospráve do 6 000 obyvateľov

jún 2025

Upozornenie

Jedným zo zadaní projektu Hodnota za peniaze je ekonomicky posudzovať plánované verejné investície a projekty. Tento materiál je hodnotením Ministerstva financií SR k zverejnenej štúdii uskutočniteľnosti. Hodnotenie pripravili pod vedením Martina Haluša a Martina Kmeťka, Michal Jerga a Jakub Karas.

Ekonomické hodnotenie MF SR má odporúčací charakter a negarantuje prostriedky z rozpočtu verejnej správy. Rozhodnutie o realizácii projektu je v kompetencii jednotlivých ministrov.

Zhrnutie

Opis projektu podľa štúdie uskutočniteľnosti

- **Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (MIRRI) plánuje zvýšiť kybernetickú bezpečnosť obcí do 6 000 obyvateľov.** Cieľom projektu má byť dosiahnutie úrovne zabezpečenia v súlade s legislatívou, minimalizácia rizika úniku osobných údajov a narušenia prevádzky IT systémov územnej samosprávy. Zavedením centralizovanej podpory pre 1 500 obcí sa má znížiť administratívna záťaž samospráv a automatizácia procesov má zrýchliť reakciu na hrozby.
- **Na splnenie minimálnych legislatívnych štandardov a školení je v projekte rozpočtovaných 1,6 mil. eur. Ďalej je plánovaný nákup, inštalácia a podpora prevádzky technologického vybavenia za 23,3 mil. eur.** Zavedenie bezpečnostných postupov zahŕňa základnú úroveň zabezpečenia obcí, napr. overenie aktuálneho stavu zabezpečenia obcí, spracovanie bezpečnostnej dokumentácie a zabezpečenie manažéra kybernetickej bezpečnosti, ktorý má byť zdieľaný medzi obcami. Nad základnú úroveň bezpečnostných služieb je plánovaný nákup hardvérového firewallu, sieťových úložísk a nástroja na monitorovanie koncových zariadení (EDR) s trojročnou licenciou a so službami na jej inštaláciu a konfiguráciu na obciach.
- **Celkové náklady projektu sú 24,9 mil. eur, z čoho sú investičné náklady 13,1 mil. eur a priemerná ročná prevádzka 1,7 mil. eur počas obdobia 7 rokov.** Investičná časť má byť hradená zo zdrojov EÚ so spolufinancovaním zo štátneho rozpočtu. Prevádzka zariadení a poplatky za licencie majú následne stáť priemerne 1,7 mil. eur ročne počas 7 rokov s predpokladaným financovaním zo štátneho rozpočtu.

Hodnotenie MF SR

- **Pre dosiahnutie úrovne bezpečnosti podľa legislatívnych požiadaviek je potrebné vypracovanie dokumentácií a postupov pre obce, ktoré majú spolu so školeniami podľa štúdie stáť 1,6 mil. eur.** Pre obce do 6 000 obyvateľov platia podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti minimálne požiadavky, ktoré spočívajú hlavne v zadefinovaní postupov pri riešení incidentov a jasného určenia zodpovednosti na úrovni predstaviteľov obce. Každá obec má tiež mať určenú pozíciu manažéra kybernetickej bezpečnosti. V projekte sa počíta s pokrytím týchto aktivít obstaraním centrálnych kapacít, ktoré budú môcť obce využívať a ktoré spolu so školeniami zamestnancov obcí majú stáť 1,6 mil. eur. Skutočná potreba môže byť nižšia, pretože časť obcí si už tieto služby zabezpečuje samostatne.
- **Plánovaný nákup a inštalácia technologického vybavenia za 23,3 mil. eur je maximálny odhad, ktorý je potrebné ďalej spresňovať na základe overenia reálneho dopytu a možností financovania dlhodobej prevádzky.** V štúdii nie je popísané, akým problémom a bezpečnostným rizikám obce čelia. Nie je preto jasné, či je nákup zariadení najefektívnejšou reakciou na reálne bezpečnostné riziká a či je aj pre veľmi malé obce potrebné nakúpiť všetky zariadenia. Potrebný počet zariadení môže byť nižší aj kvôli ich nákupu v rámci iných projektov. Detailnejšie sú obe témy popísané v bodoch nižšie:
    - **Najčastejším bezpečnostným hrozbám podľa Národného bezpečnostného úradu sa dá efektívne čeliť zavedením opatrení z prvej časti projektu.** Podľa správy NBÚ je najčastejšou hrozbou z pohľadu kybernetickej bezpečnosti phishing, teda snaha získať údaje napodobňovaním služieb, ktorým obete útoku dôverujú. Účinnou obranou proti takémuto typu útokov je hlavne zavedenie pravidelných zmien hesiel, manažment prístupov k údajom alebo bezpečnostných školení pre zamestnancov.
    - **Zálohovacie nástroje boli už pre 70 % obcí obstarané v inom projekte, nákup firewallov môže mať hlavne pre menšie obce minimálnu pridanú hodnotu.** Projekt počíta aj s nákupom 1 000 diskov slúžiacich pre zálohu dát na obciach. Nákup takýchto zariadení pre obce už bol realizovaný z iného projektu, v rámci ktorého bolo obstaraných 2 700 podobných zariadení. Firewally, ktoré MIRRI plánuje nakúpiť pre každú zapojenú obec, si už časť obcí zabezpečuje samostatne (napr. tu alebo tu). Firewall je navyše účinný len pri pripojení notebooku výhradne do obecnej siete. Jednotkové ceny, za ktoré

plánuje MIRRI zariadenia nakúpiť nie je možné overiť, na hardvér sa bežne z cenníkovej ceny poskytujú zľavy na úrovni 40 %.

- **Bez zaistenia dlhodobého financovania prevádzky za 1,7 mil. eur ročne môžu byť prínosy obmedzené na 3 roky trvania projektu.** Projekt je plánovaný na 36 mesiacov, v rámci ktorých majú väčšinu výdavkov pokryť EÚ zdroje. Následne má prevádzka a predĺženie licencií stáť 11,7 mil. eur na 7 rokov (13 % ročne z ceny investície) s predpokladaným financovaním zo štátneho rozpočtu. Bez hradenia pravidelných poplatkov za licencie a správu zariadení po skončení projektu dôjde k ukončeniu poskytovania kybernetickej bezpečnosti obcí a prínosy by boli obmedzené na obdobie 36 mesiacov. Prevádzkové náklady projektu sú tiež závislé od počtu zakúpených zariadení a licencií, preto je potrebné vypracovať postup overovania požiadaviek obcí.
- **Pre zvýšenie kybernetickej bezpečnosti je potrebné popísať, ako budú údaje z nového monitoringu koncových zariadení vyhodnocované a v praxi využívané.** Nakupované nástroje majú zabezpečiť monitoring a riešenie kybernetických incidentov. Dáta získané monitoringom je potrebné vyhodnocovať a prípadné bezpečnostné incidenty a hrozby riešiť, k čomu sú potrebné dostatočné počty bezpečnostných odborníkov. V štúdii je rámcovo popísané, že zodpovednosť za vyhodnocovanie údajov bude mať externý dodávateľ, čiastočne v spolupráci s MIRRI. Pre dlhodobé fungovanie bude potrebné zabezpečiť kapacity dlhodobo, aj po skončení projektu.
- **Pre spresnenie ekonomického hodnotenia kybernetických projektov by malo MIRRI pripraviť metodiku merania prínosov a hodnotenia rizík.** Prínosy definované v projekte sú expertný odhad MIRRI, ktorý nie je možné overiť. Na ekonomické overenie opodstatnenosti projektov na zvyšovanie kybernetickej bezpečnosti by mala vzniknúť jednotná metodika, ktorá by vychádzala z analýzy rizík pre konkrétny úrad. Následne by mali byť definované všetky alternatívy ich riešenia a vybraný nákladovo najefektívnejší variant.

Odporúčania

- Prioritne pripravovať časť projektu, ktorá je nevyhnutná pre splnenie legislatívnych požiadaviek a preškolenie zamestnancov s odhadovanými nákladmi 1,6 mil. eur.
- Pred vyhlásením verejného obstarávania spresniť rozsah rámca na nákup a inštaláciu zariadení za 23,3 mil. eur vypracovaním rizikovej analýzy a GAP analýzy. Podľa výsledkov upraviť počet nakupovaných zariadení a jednotkové ceny nastaviť na trhovú úroveň vrátane bežne poskytovaných zliav a znížiť prevádzkové výdavky na úroveň bežnú pre iné IT systémy štátu (úspora 0,8 mil. eur ročne).
- Pred podpisom zmluvy predstaviť plán dlhodobého financovania na zabezpečenie udržateľnosti kybernetickej bezpečnosti obcí aj po skončení trojročného projektu a vypracovať postup overovania požiadaviek obcí na hardvérové a softvérové zariadenia a jasne stanoviť zodpovednosť a potrebné personálne kapacity za vyhodnocovanie dát získaných z využívaných zariadení.
- Pripraviť metodiku na ekonomické hodnotenie projektov kybernetickej bezpečnosti, na základe ktorej bude možné overiť, že rozsah investície je nevyhnutný pre riešenie identifikovaných bezpečnostných rizík a bol vybraný nákladovo najviac efektívny variant riešenia.

Popis projektu

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (MIRRI) plánuje zvýšiť kybernetickú bezpečnosť obcí do 6 000 obyvateľov. Cieľom projektu má byť dosiahnutie úrovne zabezpečenia v súlade s legislatívou, minimalizácia rizika úniku osobných údajov a narušenia prevádzky IT systémov územnej samosprávy. Zavedením centralizovanej podpory sa má znížiť administratívna záťaž samospráv a automatizácia procesov má zrýchliť reakciu na hrozby.

Na splnenie minimálnych legislatívnych štandardov a školení sú v projekte rozpočtované 1,6 mil. eur. Ďalej je plánovaný nákup, inštalácia a podpora prevádzky technologického vybavenia za 23,3 mil. eur. Zavedenie bezpečnostných postupov zahŕňa základnú úroveň zabezpečenia obcí, napr. overenie aktuálneho stavu zabezpečenia obcí, spracovanie bezpečnostnej dokumentácie a zabezpečenie manažéra kybernetickej bezpečnosti, ktorý má byť zdieľaný medzi obcami. Nad základnú úroveň bezpečnostných služieb je plánovaný nákup hardvérového firewallu, sieťových úložísk a nástroja na monitorovanie koncových zariadení (EDR) s trojročnou licenciou a so službami na jej inštaláciu a konfiguráciu na obciach.

Celkové náklady projektu sú 24,9 mil. eur, investičné náklady sú 13,1 mil. eur a priemerná ročná prevádzka má stáť 1,7 mil. eur počas obdobia 7 rokov. Investičná časť sa má hradiť hlavne zo zdrojov EÚ (6,2 mil. eur) so spolufinancovaním zo štátneho rozpočtu. Od štvrtého roku projektu sa má hradiť podpora prevádzky zariadení a počíta sa aj s predĺžením licencií nástroja na monitoring koncových zariadení. Priemerné ročné výdavky na prevádzku sú odhadované na úrovni 1,7 mil. eur počas 7 rokov prevádzky s predpokladaným financovaním zo štátneho rozpočtu.

Ciele projektu

Cieľom projektu je dosiahnutie minimálnej úrovne bezpečnosti v súlade s legislatívou, minimalizácia rizika úniku osobných údajov a narušenia prevádzky systémov územnej samosprávy. Hlavný cieľ je zaistenie súladu s minimálnymi požiadavkami definovanými v zákone č. 69/2018 Z.z. o kybernetickej bezpečnosti. Cieľom je tiež zrýchliť reakciu na kybernetické hrozby, zvýšiť úroveň ochrany dát spravovaných obcami a automatizáciou procesov zrýchliť reakciu na hrozby.

Identifikácia potreby

Podľa štúdie je na splnenie legislatívnych požiadaviek prvoradé vypracovanie dokumentácií a postupov pre obce, ktoré spolu so školeniami stoja 1,6 mil. eur. Pre obce do 6 000 obyvateľov platia podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti minimálne požiadavky (kategória 1). Počíta sa hlavne so zadefinovaním postupov pri riešení incidentov a jasných určení zodpovedností na úrovni predstaviteľov obce. Každá obec má tiež mať zabezpečenú pozíciu manažéra kybernetickej bezpečnosti. V projekte sa počíta s pokrytím týchto aktivít obstaraním centrálnych kapacít, ktoré budú môcť obce využívať a ktoré spolu so školeniami zamestnancov obcí majú stáť 1,6 mil. eur. Skutočná potreba môže byť nižšia, pretože časť obcí si už tieto služby zabezpečuje samostatne (Tabuľka 1).

Tabuľka 1: Prehľad mesačných platieb za poskytovanie zákonného rozsahu kybernetickej bezpečnosti

Obec	Dodávateľ	Cena za mesiac v eur
Dubová	Osobnyudaj.sk - BA, s.r.o	90
Badín	Osobnyudaj.sk - BA, s.r.o	90
Bošáca	EP Protect s.r.o.	60
Sedlice	Dobraobec Digital s.r.o.	35

Zdroj: crz.gov.sk, webové stránky obcí, Spracovanie: ÚHP

Pre zvýšenie kybernetickej bezpečnosti je potrebné popísať, ako budú údaje z monitoringu koncových zariadení vyhodnocované a v praxi využívané. Nakupované nástroje majú zabezpečiť monitoring a riešenie kybernetických incidentov. Dáta získané monitoringom je potrebné vyhodnocovať a prípadné bezpečnostné incidenty a hrozby riešiť, k čomu sú potrebné dostatočné počty bezpečnostných odborníkov. V štúdii nie je opísaná zodpovednosť za vyhodnocovanie dát, či je na jej výkon dostatočná personálna kapacita ani spôsob reakcie pri zistení problému.

Analýza alternatív

V štúdii neboli porovnané všetky alternatívy vrátane realizácie len krokov potrebných pre splnenie legislatívnych požiadaviek. Štúdia by mala zohľadniť napr. alternatívu splnenia len zákonných požiadaviek (minimalistická), porovnania len dvoch alternatív s rovnakým rozsahom nemusí byť dostatočné. Kritériá určené na vyhodnotenie zvolených alternatív boli navyše všeobecné a bez jasnej metodiky, ako bolo ich plnenie určené. Nie je napríklad jasné, prečo by kybernetická bezpečnosť realizovaná samostatne obcami nevyhnutne viedla k nesplneniu zákonných požiadaviek.

Ekonomická analýza bola vypracovaná len pre vybranú alternatívu realizácie centrálneho projektu MIRRI. Realizácia projektu v stanovenom rozsahu ako projektu MIRRI bola jediná vyhodnotená ekonomicky, pretože iná alternatíva nesplnila kritériá v multikriteriálnej analýze. Dobrou praxou je posúdenie minimálne dvoch alternatív a vybranie alternatívy s najvyššou hodnotou za peniaze.

Tabuľka 2: Multikriteriálna analýza

Kritérium		A0: Zachovanie súčasného stavu	A1: Kybernetická bezpečnosť realizovaná obcami samostatne	A2: Kybernetická bezpečnosť realizovaná MIRRI
1	Zjednotenie štandardov, zautomatizovanie a efektivita procesov	Nie	Nie	Áno
2	Zvýšenie odolnosti voči kybernetickým incidentom a zabezpečenie kontinuity prevádzky	Nie	Nie	Áno
3	Súlad s legislatívnymi požiadavkami	Nie	Nie	Áno
4	Zníženie rizika kybernetických útokov v rámci samosprávy	Nie	Áno	Áno

Zdroj: štúdia uskutočniteľnosti, Spracovanie: ÚHP

Ekonomické hodnotenie

Celkové predpokladané náklady projektu sú vo výške 24,9 mil. eur. V rámci projektu je plánované vypracovanie a zavedenie bezpečnostných postupov a školení (1,6 mil. eur), nákupu zariadení a licencií (6,5 mil. eur) spolu s ich inštaláciou, konfiguráciou a projektovým riadením (5,4 mil. eur). Počíta sa aj so zabezpečením podpory zariadení a predĺženia licencií (11,4 mil. eur) počas siedmich rokov. Najväčšia časť nákladov má byť financovaná z vlastných zdrojov (18,6 mil. eur) s predpokladaným financovaním zo štátneho rozpočtu. Zvyšnú časť nákladov majú pokryť zdroje EÚ (6,2 mil. eur).

Efektívne riešenie najčastejších bezpečnostných hrozieb obcí sú hlavne manažment prístupov a školenia zamestnancov a nie nákup zariadení. Podľa správy NBÚ je najčastejšou hrozbou z pohľadu kybernetickej bezpečnosti phishing, teda snaha získať údaje napodobňovaním služieb, ktorým obete útoku dôverujú. Účinnou obranou proti takémuto typu útokov je hlavne zavedenie pravidelných zmien hesiel, manažment prístupov k údajom alebo bezpečnostných školení pre zamestnancov.

Plánovaný nákup a inštalácia technologického vybavenia za 23,3 mil. eur je maximálny odhad, ktorý je potrebné ďalej spresňovať na základe overenia reálneho dopytu a možností financovania dlhodobej prevádzky. V štúdii nie je popísaný spôsob výberu nakupovaných zariadení a nie je tak jasné, či sú najefektívnejšou reakciou na reálne bezpečnostné riziká. Nie je tiež dostupná analýza, aké nástroje už obce využívajú ani či si následnú prevádzku zariadení budú obce vedieť zaplatiť.

Zálohovacie nástroje boli už pre väčšinu obcí obstarané v inom projekte, nákup firewallov môže mať hlavne pre menšie obce minimálnu pridanú hodnotu. Projekt počíta aj s nákupom 1 000 diskov slúžiacich pre zálohu dát na obciach. Nákup takýchto zariadení pre obce už bol realizovaný z iného projektu, v rámci ktorého bolo obstaraných 2 700 podobných zariadení. Môže sa tak jednať o duplicitu a keďže oba projekty sú financované zo zdrojov EÚ, ich nákup nemusí byť možné z týchto zdrojov zaplatiť. Firewally, ktoré MIRRI plánuje nakúpiť pre každú obec si už časť obcí zabezpečuje samostatne (napr. tu alebo tu). Hlavne pre menšie obce je potrebné preveriť ich skutočný prínos, keďže väčšinu dát obce priamo nespravujú, ale sú v centrálnych IT systémoch (napr. IS DCOM pre výber daní alebo CISMA pre matriky) a účinnosť firewallu

bude po pripojení notebooku do inej ako obecnej siete nulová. Jednotkové ceny za ktoré plánuje MIRRI zariadenia nakúpiť nie je možné overiť, na hardvér sa bežne z cenníkovej ceny poskytujú zľavy na úrovni 40 %.

Pri zariadeniach na monitoring koncových zariadení (EDR) je potrebné zaistiť súlad projektu s činnosťami DataCentra elektronizácie územnej samosprávy SR (DEUS), ktoré vlastní väčšinu počítačov v obciach. Približne 70 % malých obcí do 6 000 obyvateľov používa výhradne počítače vo vlastníctve DEUSu. Tieto počítače sú ním centrálne spravované a bez súčinnosti MIRRI a DEUSu nie je možné projekt realizovať. EDR je bezpečnostná technológia, ktorá monitoruje a analyzuje aktivitu na zapojených počítačoch, detekuje hrozby a umožňuje reagovať v reálnom čase. Rýchla reakcia na incidenty má pomôcť minimalizovať potenciálnu škodu a zabezpečiť ochranu citlivých údajov a systémov.

Pre zvýšenie kybernetickej bezpečnosti je potrebné popísať, ako budú údaje z nového monitoringu koncových zariadení vyhodnocované a v praxi využívané. Nakupované nástroje majú zabezpečiť monitoring a riešenie kybernetických incidentov. Dáta získané monitoringom je potrebné vyhodnocovať a prípadné bezpečnostné incidenty a hrozby riešiť, k čomu sú potrebné dostatočné počty bezpečnostných odborníkov. V štúdii je rámcovo popísané, že zodpovednosť za vyhodnocovanie údajov bude mať externý dodávateľ, čiastočne v spolupráci s MIRRI. Pre dlhodobé fungovanie bude potrebné zabezpečiť kapacity dlhodobo, aj po skončení projektu.

V prípade rozhodnutia realizovať aj nákup zariadení je potrebné ich zaradiť do prevádzky čo najskôr, súčasný harmonogram počíta s inštaláciou až dva roky po obstaraní. Nákup hardvérových zariadení je plánovaný v prvom roku projektu, ale ich implementácia a konfigurácia je naplánovaná až počas tretieho roku. Hrozí tak, že nakúpené zariadenia budú dva roky na sklade a nebudú reálne obcami využívané. Životný cyklus tohto typu zariadení je spravidla približne 5-7 rokov, kedy k nim výrobca poskytuje kompletnú potrebnú podporu a aktualizácie.

Bez zaistenia dlhodobého financovania prevádzky za 1,7 mil. eur ročne môžu byť prínosy obmedzené na 3 roky trvania projektu. Projekt je plánovaný na 36 mesiacov, v rámci ktorých majú väčšinu výdavkov pokryť EÚ zdroje. Následne má prevádzka a predĺženie licencií stáť 11,7 mil. eur na 7 rokov (13 % ročne z ceny investície) s predpokladaným financovaním zo štátneho rozpočtu. Bez hradenia pravidelných poplatkov za licencie a správu zariadení po skončení projektu dôjde k ukončeniu poskytovania kybernetickej bezpečnosti obcí a prínosy by boli obmedzené na obdobie 36 mesiacov. Prevádzkové náklady projektu sú tiež závislé od počtu zakúpených zariadení a licencií, preto je potrebné vypracovať postup overovania požiadaviek obcí.

Tabuľka 3: Vplyvy na rozpočet verejnej správy (mil. eur s DPH)

Zdroj finančného krytia	2025 - 2027	2028 - 2034
Plánované investičné náklady	**13,1**	**0,0**
Z toho rozpočtovo nekrytý vplyv zo ŠR	6,9	0,0
Z toho kryté v rámci EŠIF*	6,2	-
Plánované prevádzkové náklady	**-**	**1,7****
Z toho rozpočtovo nekrytý vplyv zo ŠR	-	1,7**
Z toho rozpočtovo krytý vplyv zo ŠR	-	-

**Podľa informácií MIRRI* *Zdroj: štúdia uskutočniteľnosti, Spracovanie: ÚHP*

***Priemerne ročne*

MIRRI by malo preukázať, že centrálne zabezpečenie obcí je finančne výhodnejšie ako zabezpečenie pre každú obec samostatne. Zo štúdie nie je jasné, či obce v súčasnosti platia za kybernetickú bezpečnosť viac alebo menej, ako bude stáť centrálne poskytovanie zo strany MIRRI. Odhadované náklady projektu na prevádzku, po znížení na úroveň iných štátnych IT projektov, sú 600 eur ročne na obec.