Hodnota za peniaze projektu

Zvýšenie kybernetickej bezpečnosti samospráv do 6000 obyvateľov

september 2024

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 Andrea Kopál Srnáková.

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

- **DataCentrum elektronizácie územnej samosprávy Slovenska (DEUS) plánuje zvýšiť bezpečnostný štandard v oblasti kybernetickej a informačnej bezpečnosti pre obce do 6 000 obyvateľov.** DEUS je prevádzkovateľ centrálneho informačného systému DCOM (IS DCOM), ktorý je integrovaný na registre a databázy verejnej správy a umožňuje obciam vykonávať verejnú moc elektronicky. Projekt má zabezpečiť v obciach súlad s legislatívou o kybernetickej bezpečnosti ako aj bezpečnosť samotného IS DCOM.
- **Projekt má tri časti: nákup hardvéru a softvéru (5,1 mil. eur), zapojenie nových obcí do IS DCOM (2,3 mil. eur) a vytvorenie postupov a bezpečnostnej dokumentácie pre obce (4,8 mil. eur). Zvyšné investičné náklady na interné a externé služby sú 2 mil. eur.** Okrem nákupu hardvéru a softvéru pre dátové centrum v prvej časti projektu je plánovaný aktívny dohľad, analýza prevádzky a priebežný monitoring bezpečnosti IS DCOM. Cieľom je zamedziť výpadkom systému spôsobeným kybernetickými incidentmi a zníženie času obnovy v prípade závažného incidentu. Druhá časť projektu spočíva v zapojení ďalších 350 obcí do IS DCOM. V tretej časti projektu má byť pre zapojené obce okrem iného vypracovaná dokumentácia, nastavenie úloh a postupov riešenia kybernetických incidentov. Počíta sa aj so zapojením všetkých obcí, ktoré prejdú migráciou do IS DCOM.
- **Celková výška investičných nákladov na realizáciu projektu je odhadovaná na 14,3 mil. eur s DPH, prevádzkové náklady sú odhadované na 0,2 mil. eur ročne.** Investor očakáva hradenie investičných nákladov z najväčšej časti zo zdrojov EÚ (10,7 mil. eur), zvyšok má pokryť štátny rozpočet (2,5 mil. eur) a vlastné zdroje investora (1,1 mil. eur). Prevádzkové náklady (v priemere 0,2 mil. eur ročne na 10 rokov) majú byť hradené z vlastných zdrojov.

Hodnotenie MF SR

- **Potreba zvyšovania kybernetickej bezpečnosti v obciach vychádza hlavne z legislatívnych požiadaviek. Údaje o súčasnom stave v obciach a zvýšenom počte incidentov nie sú súčasťou štúdie.** Požiadavky na úroveň zabezpečenia IT v obciach vychádzajú zo zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Štúdia predpokladá, že obce požiadavky plošne nespĺňajú a pre ich plnenie majú nedostatočné zdroje a personálne kapacity. Skutočný stav v jednotlivých obciach ani počty incidentov štúdia nepopisuje. Potrebu zvýšiť zabezpečenie IT systémov verejnej správy konštatuje správa NBÚ o kybernetickej bezpečnosti v roku 2023, podľa ktorej je evidovaný nárast počtu bezpečnostných incidentov. Najčastejšie ide o podvodné získavanie údajov (phishing), efektívna ochrana voči nemu sú školenia a zavedené procesy (napríklad ochrana mailu, dvojfaktorové overovanie).
- **Riešenie cez centrálny projekt IS DCOM je potrebné pripraviť tak, aby nezvýšilo doplatok MF SR na prevádzku systému.** IT systém DCOM prevádzkuje združenie Datacentrum elektronizácie územnej samosprávy (DEUS), ktoré založilo a financuje Ministerstvo financií SR (MF SR) a Združenie miest a obcí (ZMOS). Časť nákladov kryje výber členských poplatkov od obcí, zvyšok dopláca MF SR. Realizáciou projektu stúpnu prevádzkové náklady systému a bez zvyšovania členských poplatkov obcí môže stúpnuť aj účasť MF SR na financovaní služieb pre obce.
- **Zapojenie aktuálne nepripojených obcí do IS DCOM má stáť 2,3 mil. eur, zvýšenie počtu zapojených obcí by malo byť súčasťou samostatného projektu.** Zapojenie obcí do IT systému DCOM je dobrovoľné, obce môžu poskytovanie elektronických služieb riešiť samostatne alebo si riešenia kúpiť od komerčných subjektov. Migrácia 350 obcí s nákladmi 2,3 mil. eur by preto nemala byť súčasťou projektu zvyšovania kybernetickej bezpečnosti. Projekt je potrebné zamerať na obce, ktoré sú už súčasťou centrálneho systému. Zapojenie ďalších obcí je potrebné podložiť záujmom obcí a realizovať v samostatnom projekte.
- **Náklady na vytváranie bezpečnostnej dokumentácie pre každú obec za 2,6 tis. eur má štúdia porovnať s cenou, za ktorú si vedia dokumentácie obce kúpiť na trhu.** Vytvorenie bezpečnostných postupov pre obce má stáť celkovo 4,8 mil. eur, náklady na jednu obec sú 2,6 tis. eur. Podľa zmlúv dostupných v centrálnom registri zmlúv (CRZ) si obce obstarávajú služby kybernetickej bezpečnosti za 18 – 72 eur mesačne, súčasťou nákladov je vytvorenie dokumentácie aj podpora pri riešení incidentov. Dokumentácie a postupy navyše môžu byť pre skupiny

obcí podobné a nie je potrebné individuálne riešenie pre každú obec. Zohľadnením ceny dostupnej na trhu, spoločným vytvorením dokumentácie a postupov a prispôsobením pre jednotlivé obce by sa mohli náklady projektu znížiť.

- **Aby inštalovaný softvér prispel k zvýšeniu bezpečnosti, získané dáta je potrebné priebežne vyhodnocovať aj po skončení projektu.** Nakupované nástroje majú zabezpečiť monitoring centrálnych komponentov IS DCOM. Dáta získané monitoringom je potrebné vyhodnocovať a prípadné bezpečnostné incidenty a hrozby riešiť, k čomu sú potrebné dostatočné počty bezpečnostných odborníkov. Na uvedený účel sú plánované 4 dodatočné personálne kapacity financované z projektu, podľa vyjadrenia DEUS sú to dostatočné kapacity na dlhodobé pokrytie všetkých potrebných aktivít.
- **Ekonomická analýza pri kybernetických projektoch by mala vychádzať z presného definovania potrebného rozsahu a spôsobu zabezpečenia s čo najnižšími nákladmi.** Kvantifikácia prínosov v štúdii je expertným odhadom. Predpoklad počtu odvrátených incidentov zavedením systému ani náklad na jeden incident nie je možné overiť. Nie sú zbierané údaje o škodách minulých incidentov, definované prínosy preto nie je možné overiť a sledovať ich naplnenie. Náklady projektu by mali byť stanovené čo najpresnejšie a potreba rôznych častí projektu dostatočne odôvodnená. Namiesto analýzy nákladov a prínosov (CBA) je preto vhodné využiť analýzu minimalizácie nákladov.

Odporúčania

- Pred vyhlásením verejného obstarávania:
    - Znížiť náklady projektu o náklady na migráciu obcí, ktoré nie sú zapojené v IS DCOM (úspora 2,3 mil. eur).
    - Uviesť, akým spôsobom budú vyhodnocované výstupy z monitorovacích nástrojov kybernetickej bezpečnosti vrátane dostupných personálnych kapacít v rámci DEUS.
    - Pred obstaraním bezpečnostnej dokumentácie (4,8 mil. eur) porovnať jednotkovú cenu s cenou na trhu, zohľadniť možnosť vypracovať len vzorovú dokumentáciu pre skupiny obcí a podľa toho upraviť náklady projektu.
- Sprístupniť dlhodobý finančný model prevádzky IS DCOM, v rámci ktorého bude možné overiť, že realizácia projektu nebude viesť k vyššiemu doplatku MF SR za služby systému pre obce.

Popis projektu

DataCentrum elektronizácie územnej samosprávy Slovenska (DEUS) plánuje zvýšiť bezpečnostný štandard v oblasti kybernetickej a informačnej bezpečnosti pre obce do 6 000 obyvateľov. DEUS je prevádzkovateľ centrálneho informačného systému DCOM (IS DCOM), ktorý je integrovaný na registre a databázy verejnej správy a umožňuje obciam vykonávať verejnú moc elektronicky. Projekt má zabezpečiť v obciach súlad s legislatívou o kybernetickej bezpečnosti ako aj bezpečnosť samotného IS DCOM.

Projekt má tri časti, prvou je nákup hardvéru a softvéru za 5,1 mil. eur, druhou je migrácia za 2,3 mil. eur. Tretia časť je vytvorenie postupov a bezpečnostnej dokumentácie pre obce za 4,8 mil. eur. Zvyšné investičné náklady na interné a externé služby sú 2 mil. eur. Okrem nákupu hardvéru a softvéru pre dátové centrum je plánovaný aktívny dohľad, analýza prevádzky a priebežný monitoring bezpečnosti IS DCOM. Cieľom je zamedziť výpadkom systému spôsobenými kybernetickými incidentmi a zníženie času obnovy v prípade závažného incidentu. Druhá časť projektu spočíva v migrácii 350 obcí do IS DCOM. V tretej časti projektu má byť pre zapojené obce okrem iného vypracovaná dokumentácia, nastavenie úloh a postupov riešenia kybernetických incidentov. Počíta sa aj so zapojením všetkých obcí, ktoré prejdú migráciou do IS DCOM.

Ciele projektu

Cieľom prvej časti projektu je zamedziť výpadkom systému spôsobenými kybernetickými incidentmi a zníženie času obnovy v prípade závažného incidentu. Bez bezpečnostnej infraštruktúry dátového centra IS DCOM by mohlo dôjsť k nedostatočnej dostupnosti systému, bezpečnostným incidentom, úniku dát alebo výpadkom, čo by závažne ovplyvnilo možnosť občanov a iných subjektov využívať elektronické služby a komunikovať s verejnými orgánmi.

Zavedením bezpečnostných opatrení v obciach (tretia časť projektu) sa má docieliť zlepšenie úrovne kybernetickej a informačnej bezpečnosti v prostredí samosprávy. V rámci druhej časti projektu sa má migráciou do IS DCOM dosiahnuť vyšší počet obcí, na ktorých bude možné realizovať aktivity priamo v obciach. Cieľom týchto aktivít je zvýšenie kybernetickej bezpečnosti a tým zamedziť napríklad narušeniu prevádzky informačných systémov obce, alebo úniku osobných údajov. Zároveň sa má zvýšiť všeobecné povedomie o téme kybernetickej bezpečnosti medzi zamestnancami a obyvateľmi samospráv.

Identifikácia potreby

Potreba zvyšovania kybernetickej bezpečnosti v obciach vychádza hlavne z legislatívnych požiadaviek, údaje o súčasnom stave v obciach a zvýšenom počte incidentov nie sú súčasťou štúdie. Požiadavky na úroveň zabezpečenia IT v obciach vychádzajú zo zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti. Štúdia predpokladá, že obce požiadavky plošne nespĺňajú a pre ich plnenie majú nedostatočné zdroje a personálne kapacity. Skutočný stav v jednotlivých obciach ani počty incidentov štúdia nepopisuje. Potrebu zvýšiť zabezpečenie IT systémov verejnej správy konštatuje správa NBÚ o kybernetickej bezpečnosti v roku 2023, podľa ktorej je evidovaný nárast počtu bezpečnostných incidentov. Najčastejšie ide o podvodné získavanie údajov (phishing), efektívna ochrana voči nemu sú školenia a zavedené procesy (napríklad ochrana mailu, dvojfaktorové overovanie).

Aby inštalovaný softvér prispel k zvýšeniu bezpečnosti, získané dáta je potrebné priebežne vyhodnocovať aj po skončení projektu. Nakupované nástroje majú zabezpečiť monitoring centrálnych komponentov IS DCOM. Dáta získané monitoringom je potrebné vyhodnocovať a prípadné bezpečnostné incidenty a hrozby riešiť, k čomu sú potrebné dostatočné počty bezpečnostných odborníkov. Na uvedený účel sú plánované 4 dodatočné personálne kapacity financované z projektu, podľa vyjadrenia DEUS sú to dostatočné kapacity na dlhodobé pokrytie všetkých potrebných aktivít.

Analýza alternatív

Alternatíva k zachovaniu súčasného stavu je okrem navrhnutého riešenia zabezpečenie kybernetickej bezpečnosti obcami samostatne. Investor v multikriteriálnej analýze (tabuľka 1) porovnal ponechanie súčasného stavu s dvomi spôsobmi zvýšenia kybernetickej bezpečnosti. Prvou možnosťou (A1) je doplnenie prvkov centrálnej infraštruktúry, migrácia obcí do IS DCOM a zavedenie bezpečnostných opatrení v obciach v navrhovanom rozsahu. Iný ako preferovaný rozsah nakupovaných komponentov a služieb sa v štúdii neposudzuje. Druhou zvažovanou alternatívou je realizácia bezpečnostných opatrení

v obciach samostatne (A2). Na základe multikriteriálnej analýzy bola alternatíva A1 bola vyhodnotená ako jediná, ktorá spĺňa všetky kritériá.

Tabuľka 1: Multikriteriálna analýza

Kritérium	A0: Zachovanie súčasného stavu	A1: Kybernetická bezpečnosť realizovaná prostredníctvom DCOM	A2: Kybernetická bezpečnosť realizovaná obcami samostatne
1 Zabezpečiť infraštruktúru ochrany dát obce v dátovom centre	Nie	Áno	Nie
2 Zníženie rizika kybernetických útokov v rámci samosprávy.	Nie	Áno	Áno
3 Zabezpečiť súlad so zákonom č. 69/2018 Z.z.	Nie	Áno	Nie
4 Efektívne vynakladanie zdrojov	Nie	Áno	Nie

Zdroj: štúdia uskutočniteľnosti, spracovanie ÚHP

Ekonomické hodnotenie

Celkové predpokladané náklady projektu sú vo výške 16,2 mil. eur. V rámci projektu sa má obstarať hardvér a softvér pre dátové centrum IS DCOM vo výške 5,1 mil. eur, náklady na migráciu obcí sú vo výške 2,3 mil. eur a vytvorenie bezpečnostnej dokumentácie je odhadnuté na 4,8 mil. eur. Zvyšné investičné náklady sú na interné a externé kapacity vo výške 2 mil. eur, prevádzkové náklady sú 1,9 mil. eur na 10 rokov. Najväčšia časť investičných nákladov má byť hradená zo zdrojov EÚ (10,7 mil. eur) a štátneho rozpočtu (2,5 mil. eur). Zvyšnú časť investičných nákladov (1,1 mil. eur) a prevádzkové náklady má pokryť investor z vlastných zdrojov. Investičné náklady je možné znížiť minimálne o 2,3 mil. eur vyňatím migrácie z projektu.

Riešenie cez centrálny projekt IS DCOM je potrebné pripraviť tak, aby nezvýšilo doplatok MF SR na prevádzku systému. IT systém DCOM prevádzkuje združenie Datacentrum elektronizácie územnej samosprávy (DEUS), ktoré založilo a financuje Ministerstvo financií SR (MF SR) a Združenie miest a obcí (ZMOS). Časť nákladov kryje výber členských poplatkov od obcí, zvyšok dopláca MF SR. Realizáciou projektu stúpnu prevádzkové náklady systému a bez zvyšovania členských poplatkov obcí môže stúpnuť aj účasť MF SR na financovaní služieb pre obce.

Rozpočet na nákup hardvéru a softvéru môže byť optimalizovaný spresnením predpokladaných cien a počtov nástrojov. Nákup centrálnej infraštruktúry pre dátové centrum IS DCOM bol hodnotený MF SR už v decembri 2023 s nákladmi 6,8 mil. eur. Po konzultácii investora s Ministerstvom investícii a regionálneho rozvoja Slovenskej republiky (MIRRI SR) a CSIRT-om sa rozsah tejto časti projektu znížil na 5,1 mil. eur. Predpokladané náklady boli stanovené prieskumom trhu. Z oslovených 16 firiem doručilo ponuky 6, z toho nie všetky zaslali ponuky na všetky položky. Výsledné náklady môžu byť od 2,7 mil. eur (pri použití minimálnych cenových ponúk) do 5,1 mil. eur (pri priemere ponúk) kvôli vysokému rozptylu. Počty nástrojov je potrebné overiť, napríklad pri 25 kusoch systému PAM (systém riadenia privilegovaných prístupov) je otázne, či má DEUS k dispozícii 25 administrátorov na jeho využitie.

Zapojenie v súčasnosti nepripojených obcí do IS DCOM má stáť 2,3 mil. eur, zvýšenie počtu zapojených obcí by malo byť súčasťou samostatného projektu. Zapojenie obcí do IT systému DCOM je dobrovoľné, obce môže poskytovanie elektronických služieb riešiť samostatne alebo si riešenia kúpiť od komerčných subjektov. Migrácia 350 obcí s nákladmi 2,3 mil. eur by preto nemala byť súčasťou projektu zvyšovania kybernetickej bezpečnosti, ktorý je potrebné zamerať na obce, ktoré sú už súčasťou centrálneho systému. Zapojenie ďalších obcí je potrebné podložiť záujmom obcí a realizovať v samostatnom projekte.

Náklady na vytváranie bezpečnostnej dokumentácie pre každú obec za 2,6 tis. eur má štúdia porovnať s cenou, za ktorú si vedia dokumentácie obce kúpiť na trhu. Vytvorenie bezpečnostných postupov pre obce má stáť celkovo 4,8 mil. eur, náklady na jednu obec sú 2,6 tis. eur. Podľa zmlúv dostupných v centrálnom registri zmlúv (CRZ) si obce obstarávajú služby kybernetickej bezpečnosti za 18 – 72 eur mesačne (box 1), súčasťou nákladov je vytvorenie dokumentácie aj podpora pri riešení incidentov. Dokumentácie a postupy navyše môžu byť pre skupiny obcí podobné a nie je potrebné individuálne

riešenie pre každú obec. Zohľadnením ceny dostupnej na trhu, spoločným vytvorením dokumentácie a postupov a prispôsobenie pre jednotlivé obce by sa mohli náklady projektu znížiť.

Box 1: Spôsoby zabezpečenia kybernetickej bezpečnosti v obciach

Obce si samostatne obstarávajú služby kybernetickej bezpečnosti často spolu s technickou podporou za desiatky eur mesačne. Súčasťou zmlúv v tabuľke 2 je vypracovanie bezpečnostnej dokumentácie, analýza a návrh bezpečnostných opatrení ako aj technická podpora pri riešení incidentov. Obce za služby platia mesačne, nedá sa presne oddeliť platba za podporu od ďalších častí zmluvy.

Tabuľka 2: Prehľad mesačných platieb za poskytovanie kybernetickej bezpečnosti

Obec	Dodávateľ	Cena za mesiac v eur
Obec Cejkov	Mahut group a.s.	72
Obec Bošáca	EP PROTECT s.r.o.	60
Obec Čaka	Dobraobec s.r.o.	30
Obec Neporadza	Dobraobec s.r.o.	24
Obed Baldovce	EP Protect s.r.o.	18
Priemer		41

Zdroj: crz.sk, spracovanie ÚHP

Ekonomická analýza pri kybernetických projektoch by mala vychádzať z presného definovania potrebného rozsahu a spôsobu zabezpečenia s čo najnižšími nákladmi. Kvantifikácia prínosov v štúdii je expertným odhadom. Predpoklad počtu odvrátených incidentov zavedením systému, ani náklad na jeden incident nie je možné overiť. Nie sú zbierané údaje o škodách minulých incidentov, definované prínosy preto nie je možné overiť a sledovať ich naplnenie. Náklady projektu by mali byť stanovené čo najpresnejšie a potreba rôznych častí projektu dostatočne odôvodnená. Namiesto analýzy nákladov a prínosov (CBA) je preto vhodné využiť analýzu minimalizácie nákladov.

Tabuľka 3: Prehľad investičných nákladov projektu

Položka	Počet	Jednotková cena (v eur)	Celková suma (v mil. eur)
DNS Firewall	14 000	101	1,4
Server	4	246 997	1,0
Web application firewall	4	167 610	0,7
Core firewall	4	126 115	0,5
EDR	2 000	191	0,4
Security Policy Automation	12	21 967	0,3
Antivírus	2 000	131	0,3
NDR	1	211 425	0,2
Vulnerability management	2 000	99	0,2
Automatické penetračné testovanie	1	113 570	0,1
PAM	25	3 476	0,1
Riadenie rizík OSS	1	37 341	0,04
Dokumentácia			4,8
Migrácia			2,3
Kapacity pre centrálnu infraštruktúru			1,1
Podporné aktivity			0,9
Prevádzka (10 rokov)			*1,9*
Kapitálové náklady spolu			***14,3***
Prevádzkové náklady spolu			***1,9***

Zdroj: štúdia uskutočniteľnosti, spracovanie ÚHP

Financovanie projektu by malo byť z najväčšej časti pokryté z fondov EÚ, pokrytie zvyšných nákladov je potrebné overiť. Zo zdrojov EÚ by malo byť pokrytých 10,7 mil. eur, DEUS má z vlastných zdrojov pokryť 1,1 mil. eur. Zvyšné investičné náklady vo výške 2,5 mil. eur majú byť kryté podľa DEUSu zo štátneho rozpočtu, čo v súčasnosti nie je možné overiť. Prevádzkové náklady (1,9 mil. eur) sú podľa štúdie vyčíslené od piateho roka vo výške 0,3 mil. eur za rok na 6 rokov a mal by ich pokryť DEUS z vlastných zdrojov.

Tabuľka 4: Vplyvy na rozpočet verejnej správy (mil. eur s DPH)

Zdroj finančného krytia	2024 - 2027
Plánované investičné náklady	14,3
Z toho kryté z fondov EÚ	10,7
Z toho rozpočtovo nekrytý vplyv zo ŠR	3,6

Zdroj: štúdia uskutočniteľnosti, spracovanie ÚHP

Citlivostná analýza a riziká projektu

Počet obcí, ktoré budú mať záujem o zabezpečenie kybernetickej bezpečnosti v rámci projektu nebol overený. Projekt počíta v rozpočte s nákladmi pre 1 805 obcí, minimálny cieľ je 1 000 obcí. Nebolo vyhodnotené, koľko obcí zapojených do IS DCOM si už obstaráva služby kybernetickej bezpečnosti samostatne. V prípade, že nebude realizovaný plný počet obcí (1 805), rozpočet by mal byť podľa štúdie lineárne ponížený.

Zabezpečenie kybernetickej bezpečnosti by malo byť dlhodobo udržateľné. V rámci projektu majú byť pre obce vypracované postupy, definovaní zodpovední zamestnanci a má byť vypracovaný plán a spôsob riešenia kybernetických incidentov.