Útvar hodnoty za peniaze

Ministerstvo financií SR / www.finance.gov.sk/uhp

Hodnota za peniaze projektu

Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov

december 2023

Upozornenie

Jedným zo zadaní projektu Hodnota za peniaze je ekonomicky posudzovať plánované verejné investície. Tento materiál je hodnotením Ministerstva financií SR k pripravovanej investícii na základe § 19a zákona 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov. Hodnotenie pod vedením Martina Haluša a Martina Kmeťka pripravili Michal Jerga a Katarína Čardášová na základe zverejnenej štúdie uskutočniteľnosti projektu.

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

Zhrnutie štúdie uskutočniteľnosti

- **Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (MIRRI SR) plánuje rozšíriť systém monitoringu kybernetických hrozieb vo verejnej správe s investičnými nákladmi 15,5 mil. eur** a priemernými prevádzkovými nákladmi 1,4 mil. eur ročne počas deviatich rokov. Na MIRRI vznikne Systém včasného varovania (EWS), ktorý bude vyhodnocovať údaje zapojených organizácií buď s vlastným bezpečnostným pracoviskom alebo využívajúcich bezpečnostné pracovisko MIRRI (Vládny SOC). Bezpečnostné pracovisko MIRRI je tiež v pláne rozšíriť a na vybrané organizácie sa zavedú nové monitorovacie nástroje.
- **Hlavným cieľom je zabezpečiť informačné systémy verejnej správy voči aktuálnym kybernetických hrozbám.** Počet závažných kybernetických bezpečnostných incidentov riešených vládnou jednotkou CSIRT (MIRRI SR) sa každoročne zvyšuje, viac než polovicu z nich predstavuje tzv. phishing, teda snaha neprávom získať údaje organizácií. Projekt má umožniť proaktívne riešenie kybernetickej bezpečnosti, centralizáciu riadenia bezpečnosti a vyššiu efektívnosť spracovania bezpečnostných údajov tak, aby boli informačné systémy zabezpečené pred kybernetickými hrozbami.
- **Potrebné nástroje vybralo MIRRI aj pre iné organizácie, vychádzalo z auditov kybernetickej bezpečnosti a rozdielovej analýzy.** Správa Národného bezpečnostného úradu (NBÚ) o stave kybernetickej bezpečnosti z roku 2022 identifikuje nesúlad s auditnými požiadavkami práve v sektore verejnej správy[1]. Rozsah projektu podľa MIRRI vychádza z výsledkov rozdielovej (GAP) analýzy na spolupracujúcich organizáciách, ktoré potvrdzujú nedostatočnú úroveň kybernetickej bezpečnosti.
- **Projekt má byť financovaný z Plánu obnovy a odolnosti (POO).** Hodnotený projekt je súčasťou Komponentu 17 Digitálne Slovensko Plánu obnovy a odolnosti Slovenskej republiky. V rámci POO investor očakáva hradenie investičných aj prevádzkových nákladov, väčšina prevádzky (10,8 mil. eur) však bude hradená zo štátneho rozpočtu.

Hodnotenie

- **Zistenia MIRRI SR a NBÚ identifikujú nárast bezpečnostných incidentov a súčasnú nedostatočnú ochranu systémov verejnej správy.** Podľa dát uvedených MIRRI bol medziročný nárast počtu incidentov v roku 2022 na úrovni 19 %. Najčastejším typom útoku je snaha o podvodné získanie údajov (tzv. phishing), efektívna ochrana voči nemu sú školenia a zavedené procesy (ochrana mailu, dvojfaktorové overovanie) bez potreby väčšej investície.
- **Nie je jasné, na aké konkrétne kybernetické hrozby reagujú zvolené nástroje a ako boli vybrané.** Navrhované nástroje sú detailne popísané z pohľadu ich vlastností a funkčnosti, dokumentácia ale neobsahuje jasné zdôvodnenie ich výberu. Výber nástrojov by mal byť realizovaný na základe reálnych údajov o súčasných bezpečnostných hrozbách a existujúceho vybavenia, na základe čoho by bolo výber možné analyticky overiť. Rozdielová analýza ani výsledky auditov nie sú súčasťou podkladov.
- **Na začiatku treba zaviesť štandardy a vzdelať zamestnancov, len nákup bezpečnostných zariadení ochranu nezvýši.** Riešenia budované centrálne nebudú úspešné bez nasadenia nových bezpečnostných zariadení na zapojených organizáciách a bez ich spolupráce tak môžu byť neefektívne. Projekt je potrebné realizovať postupne, zavádzaním štandardov a školeniami zamestnancov, až následne investovať do zariadení a programov.
- **Ekonomickú analýzu je pri kybernetických projektoch vhodnejšie pripraviť ako minimalizáciu nákladov.** Kvantifikácia prínosov 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. Namiesto analýzy nákladov a prínosov (CBA) je preto vhodné využiť analýzu minimalizácie nákladov.

[1] Národný bezpečnostný úrad

- **Rozpočet je možné znížiť o náklady na nákup hardvéru a licencií, ktorých potreba pre zvýšenie bezpečnosti nie je zdôvodnená.** Viac než tretina rozpočtu na nákup hardvéru a licencií je určená na nákup sieťovej infraštruktúry do datacentra NASES, jej súvislosť so zvyšovaním kybernetickej bezpečnosti nie je popísaná . Jej vyňatím je možné na investičných nákladoch ušetriť 4 mil. eur.
- **Prevádzkové náklady projektu pravdepodobne od roku 2027 zaťažia štátny rozpočet priemerne 1,8 mil. ročne, a preto je potrebné preveriť možnosť ich financovania z Plánu obnovy a odolnosti.** Investor počíta s úhradou časti prevádzkových nákladov zo zdrojov Plánu obnovy a odolnosti, využitie tejto možnosti v maximálnej možnej miere umožní znížiť požiadavku na štátny rozpočet.
- **Zvýšiť ekonomickú návratnosť je možné zapojením väčšieho množstva organizácií do bezpečnostného pracoviska, pokiaľ budú optimalizované dodatočné náklady na ich implementáciu.** Pri zapojení väčšieho množstva organizácií stúpne spoločenská návratnosť projektu. Ďalšie organizácie treba pripájať tak, aby boli maximálne využité vybudované technologické a personálne kapacity a dodatočné investície spojené s pripojením ďalších organizácií boli čo najnižšie.

Odporúčania

- Pred vyhlásením obstarávania:
    - Detailne odôvodniť rozsah projektu a potrebných nástrojov:
        - Zdôvodniť výber nástrojov na základe bezpečnostných hrozieb, proti ktorým sa má verejná správa brániť, a existujúceho vybavenia.
        - Sprístupniť rozdielovú (GAP) analýzu uvedenú v projekte.
    - Ekonomickú analýzu vypracovať metódou analýzy minimalizácie nákladov, nie analýzou prínosov a nákladov (CBA).
    - Znížiť rozpočet projektu o náklady na hardvér a licencie, ktorých potreba nie je zdôvodnená dosiahnutím cieľa projektu (minimálna úspora 4 mil. eur).
    - Pripraviť detailný plán implementácie, ktorý zohľadní pripravenosť organizácií využívať nasadené nástroje na monitoring a samostatne riešiť kybernetickú ochranu.
    - Overiť s NIKA ÚV SR možnosť hradenia prevádzkových nákladov projektu zo zdrojov POO do roku 2026, resp. aj po roku 2026.
    - Pripraviť usmernenie, podľa ktorého bude overovaná potreba budovať vlastné bezpečnostné pracoviská (SOC).
- V priebehu projektu:
    - Zverejniť plánovanú koncepciu o riešení bezpečnostného monitoringu pre verejnú správu vrátane budúceho zdroja financovania prevádzkových nákladov.
    - Pripraviť metodické odporúčanie pre proces zberu údajov a vyhodnocovania plnenia cieľov kybernetických projektov vo verejnej správe.
    - Na základe usmernenia pripraviť metodiku, podľa ktorej budú overované potreby budovania vlastných bezpečnostných pracovísk (SOC).

Popis, ciele a rozsah projektu

MIRR SR plánuje tromi nadväzujúcimi krokmi posilniť preventívne opatrenia v oblasti kybernetickej bezpečnosti verejnej správy s investičnými nákladmi 15,5 mil. eur. V rámci projektu sa má vybudovať Systém včasného varovania (EWS), rozšíriť služby spoločného bezpečnostného pracoviska (Vládny SOC) a tiež nakúpiť monitorovacie nástroje pre zapojené organizácie. Náklady na jednotlivé moduly sú zhrnuté v tabuľke 3.

Jednotlivé moduly a ciele na seba logicky nadväzujú. Systém včasného varovania (EWS) pre verejnú správu má umožniť zdieľanie dát z monitoringu z jednotlivých organizácií a umožniť proaktívne riešenie incidentov. Rozšírenie Vládneho SOC má šetriť personálne aj finančné zdroje organizácií v porovnaní s budovaním vlastného dohľadového centra. Počet a skladba monitorovacích nástrojov vychádzajú z bezpečnostných auditov a rozdielovej (GAP) analýzy na vybraných organizáciách.

Kybernetické projekty vo verejnej správe je potrebné riešiť koncepčne

Do plánovaného Systému včasného varovania (EWS) pre verejnú správu, ktorý je jedným z modulov posudzovaných v rámci ekonomického hodnotenia, majú byť pripojené aj novobudované rezortné bezpečnostné dohľadové pracoviská (SOC). Zriadenie rezortných SOC je financované v rámci výzvy MIRRI, ktorá je v čase písania hodnotenia v štádiu posudzovania žiadostí o dotácie.

V krátkom čase boli na hodnotenie ÚHP predložené tri projekty k zriadeniu SOC s podobnou dokumentáciou a takmer totožnými nedostatkami. Ani jeden z týchto troch projektov nie je v investičnom pláne daného ministerstva. Rovnako ani v jednom prípade nie je doložený deklarovaný nárast kybernetických incidentov, ktorý má byť dôvodom na realizáciu vlastného SOC. Zhodnotiť rozsah nakupovaného hardvéru, softvéru a licencií tak nie je možné overiť.

Tabuľka 1: Prehľad projektov budovania SOC predložených na hodnotenie ÚHP (mil. eur s DPH)

Investor	Kapitálové náklady	Prevádzkové náklady	Celkové náklady
Ministerstvo spravodlivosti SR	7,0	2,1	9,1
NCZI	6,6	1,5	8,1
DEUS	9,7	2,4	12,1
Spolu	**23,3**	**6,0**	**29,3**

Zdroj: projektové dokumentácie, spracovanie ÚHP

Projekty budovania rezortných SOC sú posudzované ešte pred zverejnením kritérií, kedy je efektívnejšie využiť služby vládneho SOC. MIRRI SR ako orgán vedenia ku kybernetických projektom má za úlohu pripraviť metodické odporúčanie so zoznamom kritérií, kedy je pre organizácie výhodnejšie potrebné vybudovať si vlastné SOC, ideálne pre celý rezort, a kedy je efektívnejšie využiť služby existujúceho Vládneho SOC. Tieto odporúčania však mali byť zverejnené ešte pred posudzovaním projektov budovania SOC. V opačnom prípade bude štát investovať do individuálnych SOC aj tam, kde to nie je potrebné, namiesto rozšírenia Vládneho SOC za zlomok nákladov.

Kybernetické projekty je potrebné koordinovať odborne a koncepčne, inak ich prevádzka neprinesie očakávanú pridanú hodnotu. Bez odborného dohľadu a koncepčného riadenia kybernetických projektov bude v najbližších rokoch zaťažovať štátny rozpočet prevádzka viacerých dohľadových centier. Pred budovaním nového dohľadového centra je nevyhnutné preukázať jeho potrebu a efektívnosť oproti riešeniu na úrovni MIRRI. V ostatných prípadoch je potrebné využiť služby Vládneho SOC alebo bezpečnostný monitoring tretích strán. Tiež je pri implementácií potrebné zabezpečiť, aby namiesto želaných „rezortných SOC“ nevznikali viaceré dohľadové centrá v rámci jedného sektora (napr. vlastný SOC pre MZ SR aj pre NCZI). Jednou z možností je do hodnotiacich kritérií výzvy na podporu projektu v kybernetickej bezpečnosti doplniť povinnosť pre podporené inštitúcie pripojiť aj ich podriadené organizácie.

Prínosy kybernetických projektov je náročné kvantifikovať a spätne overovať, nie je zavedený zber údajov a spôsob ich vyhodnocovania. Pri všetkých spomenutých projektoch boli problémom neoveriteľné prínosy, ktoré vychádzali z expertných odhadov. Je preto dôležité zaviesť metodiku, ktorá by sa zamerala na spôsob zberu údajov pre vyhodnocovanie cieľov kybernetických projektov. V ekonomickej analýze má zmysel využiť metódu minimalizácie nákladov namiesto vyhodnocovania pomeru prínosov a nákladov.

Plný potenciál projekt dosiahne len pri aktívnej spolupráci všetkých zapojených organizácií. Cieľom je zabezpečiť informačné systému verejnej správy voči kybernetickým hrozbám. Ciele majú byť dosahované so súbežne prebiehajúcimi projektami (napr. vybudovanie rezortných SOC). Pre dosiahnutie želaného výsledku je nevyhnutná koordinácia projektov a ich prepojenie.

Porovnanie alternatív

V štúdii uskutočniteľnosti sú identifikované 3 alternatívy riešenia súčasného stavu. Investor v multikriteriálnej analýze (tabuľka 2) porovnal ponechanie súčasného stavu (A0) s rôznymi spôsobmi zabezpečenia bezpečnostného monitoringu. Prvou možnosťou (A1) je zavádzanie služieb bezpečnostných nástrojov a monitoringu priamo internými kapacitami organizácií decentralizovanie. Ďalej bola preskúmaná možnosť zazmluvnenia tretích strán, ktoré by organizáciám poskytovali „SOC as a service", súčasné služby VJ CSIRT by sa nerozširovali. Treťou alternatívou (A3) je budovanie centralizovaného riešenia formou rozvoja existujúceho Vládneho SOC. Zároveň budú na vybrané organizácie nasadzované technológie pre zber údajov. Preferovaným riešením, ktoré vstupuje do ekonomickej analýzy (CBA), je alternatíva 3.

Tabuľka 2: Multikriteriálna analýza

Kritérium	A0: Zachovanie súčasného stavu	A1: Interné kapacity a decentralizácia	A2: Externé služby monitoringu a existujúce služby VJ CSIRT	A3: Centralizácia poskytovania služieb od NASES a VJ CSIRT
1 Budovanie vybavenie	Nie	Čiastočne	Áno	Áno
2 Efektívne spracovanie bezpečnostných udalostí	Nie	Nie	Áno	Áno
3 Efektívny manažment informácií	Nie	Čiastočne	Čiastočne	Áno
4 Zvýšenie zabezpečenia IS v prostredí VS	Nie	Čiastočne	Áno	Áno
5 Efektívne využívanie dát s cieľom včasného varovania	Nie	Nie	Nie	Áno

Zdroj: projektová dokumentácia, spracovanie ÚHP

V štúdii nie sú rozpracované alternatívy realizácie len časti modulov, dôvodom má byť ich previazanosť. Jednou z technických možností je vynechanie realizácie Systému včasného varovania (EWS). Jeho vytvorenie je však jedným zo zámeru projektu, na ktorý sú naviazané kvantifikované prínosy. Taktiež je jedným z definovaných cieľov Plánu obnovy a odolnosti. Potenciál tohto systému bude môcť byť naplno využívaný len pri úspešnej realizácii sektorových SOC, a zároveň aktívnej spolupráce organizácií zapojených do vládneho SOC. Je preto potrebné dbať na úspešnú implementáciu jednotlivých častí projektu.

Dopyt

Verejná správa vykazuje nedostatočné výsledky súladu s auditnými požiadavkami na kybernetickú bezpečnosť. Podľa výsledkov auditu NBÚ má verejná správa nedostatky pri zabezpečovaní kybernetickej bezpečnosti. Subjekty verejnej správy zvyšujú úroveň kybernetickej bezpečnosti vo svojej organizácii najmä z dôvodu legislatívnych požiadaviek, pričom väčšina subjektov neimplementuje opatrenia nad rámec povinností. Výsledky auditu tiež ukazujú, že organizácie často nemajú k dispozícii postupy či schopnosti na zvládanie eventuálnych incidentov.

Väčšina organizácií nemá zabezpečený bezpečnostný monitoring, ostatné využívajú najmä externé služby monitoringu alebo prevádzkujú vlastné bezpečnostné dohľadové centrum. Spravidla menšie organizácie využívajú služby tretích strán pre zabezpečenie bezpečnostného monitoringu, pričom sú pokrývané vybrané segmenty kybernetickej bezpečnosti. Iba niekoľko organizácií s komplexnejšou infraštruktúrou už v súčasnosti prevádzkuje vlastné bezpečnostné dohľadové centrá. Limitom ich zriaďovanie sú vysoké náklady a nedostatok špecialistov na kybernetickú bezpečnosť.

Problémy oboch súčasných riešení monitoringu má projekt čiastočne vyriešiť rozšírením Vládneho SOC. Jedným z častí projektu je aj koncentrácia personálnych a finančných zdrojov do rozšírenia Vládneho SOC, kam budú v prípade záujmu pripájané subjekty verejnej správy. Tým sa tak rozšíria segmenty kybernetickej bezpečnosti,

ktoré budú monitorované, a zároveň nebudú musieť z vlastných zdrojov hradiť vybudovanie vlastného dohľadového centra či robiť nábor špecialistov, ktorých je na trhu nedostatok.

Ekonomické hodnotenie

V rámci projektu sa obstarávajú hardvér (5,4 mil. eur), softvér a licencie (5,3 mil. eur) a nový systém (4,7 mil. eur). Prevádzkové náklady sú vo výške 12,2 mil. eur počas 9 rokov, investor ich plánuje hradiť čiastočne zo zdrojov POO. V budúcnosti má byť zdroj ich financovania upravený v novej koncepcii, časť nákladov by znášali samotné pripájané organizácie. Ciele a prínosy projektu je možné dosiahnuť len pri úspešnej implementácie jednotlivých častí projektu na rôznych organizáciách. Ekonomickú návratnosť je možné zvýšiť optimalizáciou nákladov hardvér a licencie, ako aj zapojením viacerých organizácií do Vládneho SOC.

Rozpočet na obstaranie vybavenia môže byť optimalizovaný znížením neopodstatnených výdavkov na hardvér a licencie. Viac než tretinu nákladov na hardvér a licencie tvorí položka vizualizačnej platformy pre NASES (4 mil. eur). Počet a skladba zvolených nástrojov nakupovaných pre organizácie a rozšírenie Vládneho SOC neboli zdôvodnené, je možný priestor na ich optimalizáciu. Prioritne je potrebné vyhodnotiť, ako boli zvolené nástroje s ohľadom na typ a počet kybernetických incidentov.

Ekonomickú návratnosť zvýši aj väčší počet organizácií zapojených do Vládneho SOC a Systému včasného varovania (EWS). Prínosy projektu budú dosiahnuté, len ak sa podarí pripojiť dostatočný počet organizácií do Vládneho SOC, ktoré budú aktívne aj samostatne zapracovávať opatrenia z auditu. Zároveň sa do EWS majú pripojiť aj organizácie s vlastným novým SOC. Niektoré organizácie takéto pracovisko už prevádzkujú, ďalšie sú len v procese hodnotenia projektovej dokumentácie. Zvýšením počtu organizácií zapojených do Vládneho SOC a EWS je možné ďalej zvýšiť ekonomickú návratnosť projektu, pokiaľ budú maximálne využité personálne a technologické kapacity.

Projekt počíta s využitím rámcovej zmluvy a dynamického nákupného systému. Súčasne nastavené HW/SW kapacity sú prepočítané pre sedem nových organizácií, pričom pri šiestich z nich už boli začaté diskusie k pripojeniu do Vládneho SOC. Zároveň sa rozširujú HW kapacity na centrálnej úrovni SOC, ktoré umožnia pripájanie ďalších organizácií po ukončení projektu. Obstaranie hardvéru na Vládny SOC pre budúce organizácie by malo prebehnúť až po overení skutočného záujmu organizácii o pristúpenie do centrálneho riešenia. Zároveň je potrebné overiť možnosti týchto organizácií samostatne pracovať na ochrane pred kybernetickými hrozbami.

Prevádzkové náklady počas trvania projektu majú byť hradené z rozpočtu POO, možnosťou je aj nový model spoplatnenia služieb Vládneho SOC. Po ukončení projektu majú byť prevádzkové náklady hradené zo zdrojov štátneho rozpočtu (10,7 mil. eur). V budúcnosti sa počíta s modelom, kedy by časť prevádzkových nákladov súvisiaca s nástrojmi nasadenými na jednotlivé organizácie bola hradená samotnými organizáciami. Úprava takejto možnosti má byť predstavená v pripravovanej koncepcii o riešení bezpečnostného monitoringu pre verejnú správu.

V rozpočte nie sú vyčíslené vyvolané náklady pre organizácie, ktoré budú zapojené do Vládneho SOC. Na strane organizácií bude v súlade so zisteniami auditu zapracovať rôznorodé odporúčania, ktoré sú podmienkou pre pripojenie sa do Vládneho SOC. Zapracovanie zistení z auditu by však musela organizácia znášať aj bez pripojenia do centrálneho riešenia. Vyvolanými nákladmi tak zostávajú náklady na energie a priestor v serverovni. Na druhej strane organizáciám vo Vládnom SOC odpadnú náklady na antivírus, monitorovacie nástroje a služby SOC, ktorými organizácie musia disponovať podľa zákona o kybernetickej bezpečnosti.

Tabuľka 3: Celkové náklady projektu (mil. eur s DPH)

Položka	Systém včasného varovania (EWS)	Vládny SOC	Nástroje pre pripájané organizácie
Aplikácia	1,1	1,4	2,3
Softvér	1,2	0,3	3,7
Hardvér	0,3	3,7	1,4
Riadenie projektu	0,02	0,03	0,05
Prevádzka (9 rokov)	2,4	3,4	6,4

Kapitálové náklady spolu	**15,5**
Prevádzkové náklady spolu	**12,2**

Zdroj: projektová dokumentácia, spracovanie ÚHP

Analýza rizík

Úspešnosť projektu závisí od spolupráce s jednotlivými zapojenými organizáciami. Ciele projektu aj prínosy projektu sú závislé na spolupráci organizácií a úspešnosti ďalších súbežných projektov pri zriaďovaní sektorových SOC. Pokiaľ organizácie nebudú aj samostatne pracovať na zapracovaní zistení z auditu NBÚ, ich pripojenie do Vládneho SOC nebude efektívne. Do systému včasného varovania (EWS) majú byť okrem Vládneho SOC zapojené aj nové rezortné SOC, ktoré sú v štádiu hodnotenia projektovej dokumentácie. Prínosy EWS tak budú môcť byť dosiahnuté až neskôr v čase.

Vládny SOC sa bude neustále rozširovať, čo znamená pravidelné zvýšenie nárokov na štátny rozpočet. Súčasný rozsah nákupu je určený pre sedem jednoduchšie implementovaných organizácií. V čase má počet organizácií zapojených do Vládneho SOC narastať. MIRRI SR by preto už v súčasnosti malo pracovať na nastavení takého modelu financovania, ktorý nebude plne odkázaný na financovanie zo štátneho rozpočtu.

Vyvolané náklady organizácií zapojených do Vládneho SOC nie sú známe. Časť nákladov by organizáciám vznikla aj bez zapojenia sa do Vládneho SOC, nakoľko zistenia z auditu NBÚ by museli zapracovať nezávisle od projektu. Avšak, časť personálnych nákladov organizácií môže byť ovplyvnená pripojením sa do Vládneho SOC. Zároveň organizáciám odpadá časť nákladov na hardvér či softvér. Presný pomer nákladov a úspor z pohľadu zapojených organizácií z dokumentácie nie je jasný, je potrebné ho aktualizovať po pilotnom riešení pripojenia prvých organizácií.