

Centrálny systém proaktívnej kybernetickej ochrany (CSPKO)

Hodnota za peniaze projektu

september 2026

Upozornenie

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

Ekonomické hodnotenie Ministerstva financií Slovenskej republiky má odporúčací charakter a negarantuje prostriedky z rozpočtu verejnej správy. Rozhodnutie o realizácii projektu je v kompetencii jednotlivých ministrov.

Opis projektu podľa štúdie uskutočniteľnosti

- **Vládna jednotka CSIRT (VJ CSIRT)** spadajúca pod Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (MIRRI) **plánuje rozšíriť centrálné poskytované služby kybernetickej bezpečnosti**. Podľa štúdie *nemusia mať všetky organizácie vybudované personálne a technické kapacity na zabezpečenie kybernetickej ochrany, a úroveň zabezpečenia preto môže byť nerovnomerná alebo nedostatočná. Vzniknuté bezpečnostné incidenty sa zároveň majú riešiť prevažne reaktívne a len málo kapacity sa venuje ich predchádzaniu. Podľa štúdie predstavitelia viacerých obcí a organizácií na stretnutiach prejavili záujem o využitie týchto služieb. Navrhované posilnenie centralizovaných služieb poskytovaných CSIRT tak má zvýšiť pravdepodobnosť úspešnej obrany proti útokom a zároveň znížiť čas a náklady na odstránenie škôd po úspešných útokoch.*
- **Cieľom je zvýšiť úroveň kybernetickej ochrany v štáte, pričom VJ CSIRT má byť schopná kontrolovať riziká v rámci iných organizácií a analyzovať charakter hrozieb.** VJ CSIRT bude po realizácii projektu schopná organizáciám verejnej správy dôkladnejšie kontrolovať zabezpečenie ich sietí a systémov, aby sa slabé miesta odhalili skôr, než ich zneužije útočník. Pribudnúť má tiež služba včasného varovania pred hrozbami, ktorá by mala umožniť rýchlejšiu identifikáciu kybernetického incidentu. V prípade napadnutia bude viesť VJ CSIRT postihnutej organizácii poskytnúť náhradný spôsob komunikácie, pomôcť jej bezpečne obnoviť dáta a systémy a nájsť a odstrániť útočníkov, ktorí sa v sieti skrývajú už dlhší čas. Na zabezpečenie týchto služieb plánuje MIRRI nakúpiť okrem softvérových nástrojov aj hardvér vo forme incidentového úložiska. Úložisko má okrem interných potrieb VJ CSIRT slúžiť aj na poskytovanie služieb bezpečnej obnovy dát a kontroly škodlivého kódu v súboroch.
- **Investičné náklady projektu sú odhadované na 23,5 mil. eur, celkové náklady počas 10 rokov majú dosiahnuť 35,8 mil. eur.** V rámci investície sa počíta s nákupom hardvéru za 19,4 mil. eur a nákup softvéru je plánovaný vo výške 4,1 mil. eur. Ročná prevádzka riešenia má stáť 0,4 mil. eur ročne. Okrem počiatočnej investície do hardvéru je plánovaná aj jeho modernizácia za 8 mil. eur po štyroch rokoch prevádzky.

Hodnotenie MF SR

- **MIRRI SR navrhlo rozšíriť centrálné poskytované kybernetické služby bez overenia záujmu organizácii verejnej správy o ich využívanie.** Centralizácia má zmysel vtedy, ak si organizácie nevedia potrebné služby zabezpečiť samy alebo je výhodnejšie ich zabezpečovať centrálné, ako keď je výkon ponechaný na samotné organizácie. Druh a rozsah služieb navrhovaných v projekte ale nevychádza z analytického overenia dopytu a analýzy súčasného stavu a nemusí byť vhodné ich centralizovať. Časť väčších organizácií už prevádzkuje vlastné riešenia na zabezpečenie kybernetickej bezpečnosti a tak by o centralizované služby nemuseli mať záujem. Menšie organizácie a obce tieto služby nemusia potrebovať v takom rozsahu, ako sú v štúdiu plánované.
- **Pred rozhodnutím o pokračovaní projektu by preto mala štúdia pri jednotlivých službách najprv overiť skutočný dopyt a podložiť ich prínosy na reálnych prevádzkových dátach.** Štúdia navrhuje vytvorenie viacerých služieb v rámci VJ CSIRT, ktoré majú zvýšiť bezpečnosť organizácií. Ani pri jednej neobsahuje údaje o tom, či ich úrady už nemajú zabezpečené resp. že by ich v prípade zavedenia plánovali využívať a služby by reagovali na hrozby, ktorým v praxi čelia. Pred rozhodnutím rozšíriť služby by preto štúdia mala preukázať, že úrady budú rozšírené centrálné služby využívať a ich zameranie zodpovedá skutočným hrozbám. Zavedenie nových služieb tiež nemusí priniesť štátu viac benefitov v porovnaní s potrebnými nákladmi. Výpočet prínosov totiž vychádza z expertných a neoveriteľných predpokladov a už pri ich malej zmene (napr. ak zabráni ročne 5 veľkým incidentom namiesto očakávaných 6) nebude projekt ekonomicky návratný. Štúdia by preto mala výhodnosť investície do jednotlivých služieb preveriť samostatne a na základe overiteľných historických údajov, napr. pri službe na kontrolu kompromitácie záloh preukázaním počtu prípadov, kedy hrozilo využitie napadnutých dát s rizikom ďalších škôd.
- **V nadväznosti na konečné rozhodnutie o rozšírení služieb je potrebné upraviť rozsah obstarávaného hardvéru a softvéru, najmä kapacitu hardvérového úložiska za 19,4 mil. eur.** Najväčšou položkou investície (80 % nákladov) je obstaranie incidentového úložiska, ktoré má slúžiť pre potreby viacerých plánovaných služieb. Jeho kapacita bola v priebehu hodnotenia znížená z 1,5 PB na 1 PB. Štúdia ale stále neobsahuje údaje a prepočty na

overenie, či je takáto kapacita skutočne potrebná a bude v praxi využitá. Najmenej 70 % kapacity je zároveň vyhradenej pre služby, ktorých prínosy a záujem úradov ich využívať by ešte mala štúdia podložiť. Náklady incidentového úložiska priamo súvisia s jeho navrhovanou úložnou kapacitou, preto je nevyhnutné odhad kapacity spresniť a podložiť overiteľnými prepočtami. Štúdia by zároveň mala opísať aj možnosť postupného rozširovania úložiska podľa potreby a nepočítať výlučne s nákupom plnej kapacity na začiatku projektu.

- **Aj v prípade, že sa incidentové úložisko obstará v pôvodnom rozsahu, je možné odhad nákladov znížiť o 5,1 mil. eur využitím najnižšej ponuky z prieskumu trhu.** MIRRI v rámci prieskumu dostalo tri ponuky, rozdiel medzi najvyššou a najnižšou ponukou pre incidentové úložisko je viac ako 9 mil. eur. MIRRI nevysvetľuje, prečo za najlepší možný odhad trhovej ceny považuje priemer ponúk, keď jeden z oslovených dodávateľom je ochotný dodať riešenie za výrazne nižšiu cenu. Určenie predpokladanej ceny na úrovni najnižšej ponuky umožňuje a zákon o verejnom obstarávaní. MIRRI sa navyše podľa štúdie rozhodlo na zabezpečenie nových softvérových služieb používať iba komerčné riešenia, použitie a prispôbenie open source alebo bezplatných riešení (napr. [THOR Lite](#) či [Velociraptor](#)) však môže byť lacnejšie a štúdia by mala vyhodnotiť efektívnosť ich používania oproti len komerčným riešeniam.
- **Pred rozširovaním služieb je potrebné potvrdiť, že všetky budúce náklady budú kryté v rámci limitu kapitoly MIRRI a projekt nebude vyžadovať navýšenie personálnych kapacít CSIRT.** Počiatočná investícia má byť realizovaná zo zdrojov EÚ, náklady na obnovu hardvéru vo výške 8 mil. eur majú byť hradené zo štátneho rozpočtu. Pred rozhodnutím obstaráť hardvér by malo MIRRI potvrdiť, že bude vedieť pokryť aj jeho obnovu bez dodatočnej požiadavky na štátny rozpočet. V štúdii sa tiež uvádza, že zavedenie nových služieb nebude vyžadovať zvýšené personálne náklady, CSIRT by ale mal pred realizáciou projektu preukázať, že bude schopný rozšírené služby poskytovať aj so súčasnými personálnymi kapacitami aj pri očakávanom zvýšení dopytu.

Odporúčania

- Pred rozhodnutím realizovať projekt analyticky overiť záujem organizácii verejnej správy o používanie nových a rozšírených služieb.
- Realizovať len služby s potvrdenými prínosmi na základe reálnych dát a overiteľného prepočtu, aké výhody zavedenie nových služieb štátu prinesie.
- Pred nákupom incidentového úložiska upresniť jeho potrebnú kapacitu podľa realizovaných služieb a preveriť možnosť jeho postupného rozširovania.
- Pri obstarávaní aktuálne navrhovanej kapacity nastaviť predpokladanú hodnotu na úrovni najnižšej ponuky (úspora 5,1 – 13,6 mil. eur).
- Potvrdiť, že pri nákupe hardvéru bude MIRRI schopné zaplatiť aj jeho plánovanú obnovu za 8 mil. eur v rámci udržateľnosti projektu bez dodatočnej požiadavky na štátny rozpočet.

Popis projektu

MIRRI plánuje obstarat' rozšírenie technológií centrálne poskytovaných služieb kybernetickej bezpečnosti. Navrhovaná investícia má byť podľa štúdie reakciou na výrazný nárast závažných kybernetických bezpečnostných incidentov v posledných rokoch a zhoršujúcu sa situáciu v oblasti kybernetickej bezpečnosti. Projekt má zároveň podporiť napĺňanie strategickej priority 5 Kybernetická a informačná bezpečnosť podľa [NKIVS 2025](#).

VJ CSIRT poskytuje viacero centrálnych služieb na zabezpečenie kybernetickej bezpečnosti, tie sú však podľa štúdie na nedostatočnej úrovni. Centrálné služby majú zabezpečovať len časť potrebnej ochrany, zvyšok je ponechaný na organizácie verejnej správy. Mnohé organizácie ale nemajú vybudované kapacity na zabezpečenie kybernetickej ochrany, a tak je úroveň zabezpečenia nerovnomerná a v mnohých prípadoch nedostatočná. Vzniknuté bezpečnostné incidenty sa zároveň riešia prevažne reaktívne a len málo kapacity sa venuje ich predchádzaniu. Posilnenie centralizovaných kapacít tak má zvýšiť pravdepodobnosť úspešnej obrany proti útokom a zároveň znížiť čas a náklady na odstránenie škôd po úspešných útokoch.

Celkové náklady projektu majú dosiahnuť 35,8 mil. eur s DPH. Počiatočné investičné náklady sú vo výške 23,5 mil. eur, z toho nákup hardvéru tvorí 19,4 mil. eur a nákup softvéru je plánovaný vo výške 4,1 mil. eur. Ročná prevádzka riešenia má stáť 0,4 mil. eur ročne. Okrem počiatočnej investície do hardvéru je plánovaná aj jeho modernizácia za 8 mil. eur po štyroch rokoch prevádzky.

Ciele projektu

Cieľom je zvýšiť úroveň kybernetickej ochrany v štáte, pričom VJ CSIRT má byť schopná kontrolovať riziká v rámci iných organizácií a analyzovať charakter hrozieb. VJ CSIRT bude po realizácii projektu schopná organizáciám verejnej správy dôkladnejšie kontrolovať zabezpečenie ich sietí a systémov, aby sa slabé miesta odhalili skôr, než ich zneužije útočník. Pribudnúť má tiež služba včasného varovania pred hrozbami, ktorá by mala umožniť rýchlejšiu identifikáciu kybernetického incidentu. V prípade napadnutia bude viesť VJ CSIRT postihnutej organizácii poskytnúť náhradný spôsob komunikácie, pomôcť jej bezpečne obnoviť dáta a systémy a nájsť a odstrániť útočníkov, ktorí sa v sieti skrývajú už dlhší čas. Na zabezpečenie týchto služieb plánuje MIRRI nakúpiť okrem softvérových nástrojov aj hardvér vo forme incidentového úložiska. Úložisko má okrem interných potrieb VJ CSIRT slúžiť aj na poskytovanie služieb bezpečnej obnovy dát a kontroly škodlivého kódu v súboroch.

Identifikácia potreby

MIRRI navrhlo rozšíriť centrálne poskytované služby bez analytického overenia záujmu organizácii verejnej správy o ich využívanie. Centralizácia má zmysel vtedy, ak si organizácie nevedia potrebné služby zabezpečiť samy alebo je výhodnejšie ich zabezpečovať centrálne, ako keď je to ponechané na samotné organizácie. Druh a rozsah navrhovaných služieb ale nevychádza z overeného dopytu a nemusí byť potrebné ich centralizovať. Časť väčších organizácií však už vlastné riešenia na zabezpečenie kybernetickej bezpečnosti prevádzkuje a tak by o centralizované služby nemuseli mať záujem. Podľa štúdie existuje anekdotálny dopyt zo strany niektorých obcí a organizácií, ten však nie je analyticky zmapovaný. Menšie organizácie a obce tieto služby nemusia potrebovať v takom rozsahu, ako sú v štúdii plánované. Súčasťou štúdie je štatistický podložený nárast závažných incidentov, no chýba hlbšia analýza povahy a príčin týchto incidentov a najvhodnejších spôsobov ich predchádzania alebo riešenia. Aj podľa [zákona o kybernetickej bezpečnosti](#) majú byť bezpečnostné opatrenia prijímané na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti.

Z podkladov nie je zrejmé, či je záujem organizácií o používanie plánovaných nástrojov a služieb overený. Štúdia navrhuje vytvorenie viacerých služieb v rámci CSIRT, ktoré majú zvýšiť bezpečnosť úradov. Ani pri jednej neobsahuje údaje o tom, že ich úrady už nemajú zabezpečené resp. že by ich v prípade zavedenia plánovali využívať a služby by reagovali na hrozby, ktorým v praxi čelia. Pred rozhodnutím rozšíriť služby by preto štúdia mala preukázať, že úrady budú rozšírené centrálné služby využívať a ich zameranie zodpovedá skutočným hrozbám. Nie je zrejmé, do akej miery bude centralizované riešenie duplicitné napr. s už obstaranou [Platformou na podporu kybernetickej bezpečnosti MV SR](#).

Analýza alternatív

Štúdia uskutočniteľnosti neobsahuje porovnanie open source a bezplatných nástrojov s vybranými komerčnými riešeniami, napriek tomu, že ich použitie môže byť efektívnejšie. V štúdii sa na základe vymenovania nevýhod open-source nástrojov vylučuje použitie týchto nástrojov, zároveň sa v štúdii konštatuje, že VJ CSIRT niektoré open-source riešenia používa už teraz (napr. softvérovú platformu [MISP](#)). Použitie a prispôbenie open source alebo bezplatných riešení (napr. [THOR Lite](#) či [Velociraptor](#)) však môže byť efektívnejšie a malo byť súčasťou porovnania alternatív.

Ekonomické hodnotenie

Pred rozhodnutím o pokračovaní projektu by mala štúdia pri jednotlivých službách najprv overiť skutočný dopyt a podložiť ich prínosy na reálnych prevádzkových dátach. Súčasný výpočet prínosov je totiž len veľmi hrubý odhad, postavený na kombinácii prevzatých medzinárodných benchmarkov a expertných odhadov VJ CSIRT. Napríklad veľké incidenty majú mať pri zavedení jednej z nových služieb v priemere o 22% menší finančný dopad, tento odhad ale v štúdii nie je ničím podložený. Štúdia by preto mala výhodnosť investície do jednotlivých služieb preveriť samostatne a na základe overiteľných historických údajov, napr. pri službe na kontrolu kompromitácie záloh preukázaním počtu prípadov, kedy hrozilo využitie napadnutých dát s rizikom ďalších škôd.

Najväčšiu investičnú časť projektu tvorí nákup incidentového úložiska za 19,4 mil. eur a jeho obnova po piatich rokoch za 8 mil. eur, jeho kapacita však nemusí byť využitá. Polovica úložiska (500 TB) má byť alokovaná na služby bezpečnej obnovy údajov, ktoré majú organizácie využívať ako alternatívne záložné úložisko pri kybernetických incidentoch. Podľa predložených podkladov zo strany VJ CSIRT by na naplnenie tejto kapacity museli v jednom čase nahrať svoju dáta dve až tri väčšie ministerstvá, pri tých je však predpoklad, že záložné úložiská majú už vybudované a služby by teda pravdepodobne nevyužili. Menšie úrady a organizácie podľa podkladu VJ CSIRT vo všeobecnosti spravujú menej dát, aj v prípade záujmu o využitie služieb by teda plánovanú kapacitu zrejme nenaplnili. Na ďalšiu novú službu, overovanie súborov a kódu, má byť alokovaná takmer tretina úložiska (300 TB), dopyt po nej nie je overený. Aj v prípade overeného dopytu sa však dá predpokladať, že by táto kapacita bola nebola plne využitá, keďže na jej plné využitie by bolo potrebné nahrať 60 miliónov 5 MB súborov denne. Súčasťou investície majú byť aj dva mobilné systémy na prenos dát pri incidentoch s celkovou kapacitou 200 TB, z podkladov však nie je zrejme, prečo majú byť takéto systémy dva a ako bola určená ich potrebná kapacita.

Aj v prípade, že sa úložisko obstará v pôvodnom rozsahu, je možné odhad nákladov znížiť o 5,1 mil. eur využitím najnižšej ponuky z prieskumu trhu. MIRRI v rámci prieskumu dostalo tri ponuky, rozdiel medzi najvyššou a najnižšou ponukou pre incidentové úložisko je viac ako 9 mil. eur. MIRRI nevysvetľuje, prečo za najlepší možný odhad trhovej ceny považuje priemer ponúk, keď jeden z oslovených dodávateľom je ochotný dodať riešenie za výrazne nižšiu cenu. Určenie predpokladanej ceny na úrovni najnižšej ponuky umožňuje a zákon o verejnom obstarávaní. MIRRI sa navyše podľa štúdie rozhodlo na zabezpečenie nových softvérových služieb používať iba komerčné riešenia, použitie a prispôbenie open source alebo bezplatných riešení (napr. [THOR Lite](#) či [Velociraptor](#)) však môže byť lacnejšie a štúdia by mala vyhodnotiť, či ich využitie môže byť efektívnejšie.

Plánovaný rozsah nákupu softvérových nástrojov je potrebné spresniť podľa dopytu zo strany organizácii. Napr. pri rozšírení služby preventívneho skenovania zraniteľností na 1000 licencií nie je zrejmé, koľko z organizácií túto službu potrebuje a nevie si ju samostatne zabezpečiť. Ďalších 1000 licencií má byť záložných, z toho 500 ako pohotovostná kapacita pri závažných incidentoch a 500 na reaktívne skenovanie na vyžiadanie. Tieto však nemusia byť vôbec využité, resp. nie je zrejmé, prečo by rozsah nemohol byť napr. len polovičný, keďže ide o služby na vyžiadanie. Rovnako to platí pre službu tzv. threat hunting a služby „deception“, počet potrebných licencií nie je možné na základe dodaných podkladov overiť.

Pred rozširovaním služieb je potrebné potvrdiť, že všetky budúce náklady budú kryté v rámci limitu kapitoly MIRRI a projekt nebude vyžadovať personálnych kapacít CSIRT. Počiatočná investícia má byť realizovaná zo zdrojov EÚ, náklady na obnovu hardvéru vo výške 8 mil. eur majú byť hradené zo štátneho rozpočtu. Pred rozhodnutím obstaráť hardvér by malo MIRRI potvrdiť, že bude vedieť pokryť aj jeho obnovu bez dodatočnej požiadavky na štátny rozpočet. V štúdii sa tiež uvádza, že zavedenie nových služieb nebude vyžadovať zvýšené personálne náklady, CSIRT by ale mal pred realizáciou projektu preukázať, že bude schopný rozšírené služby poskytovať aj so súčasnými personálnymi kapacitami aj pri očakávanom zvýšení dopytu.