Platforma na podporu kybernetickej bezpečnosti

Hodnota za peniaze projektu

november 2025

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 Haluša a Martina Kmeťka, Michal Jerga a Daniel Mušec.

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.

Zhrnutie

Opis projektu podľa štúdie uskutočniteľnosti

- **Ministerstvo vnútra SR (MV SR) plánuje obstarať platformu kybernetickej bezpečnosti založenú na technológii umelej inteligencie (AI).** Projekt má byť realizovaný nákupom licencií technológie, ktorá využíva modely prediktívnej detekcie kybernetických hrozieb s pomocou AI. Navrhovaná investícia má byť reakciou na zvýšený počet kybernetických incidentov a útok na systémy slovenského katastra nehnuteľností z januára 2025.
- **Cieľom projektu je posilniť odolnosť informačných systémov a digitálnej infraštruktúry pre 10 vybraných organizácií voči kybernetickým hrozbám a podporiť schopnosti kybernetickej ochrany a obrany.** Platforma má zabezpečiť jednotný dohľad nad IT infraštruktúrou viacerých organizácií a automatizovanú reakciu na prípadné hrozby. Podľa MV SR má projekt naplniť legislatívne požiadavky európskej smernice o kybernetickej bezpečnosti NIS 2 a zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, konkrétne v sektore 6.3 Digitálna infraštruktúra a 8.1 Verejná správa.
- **Celkové náklady projektu 62,4 mil. eur s DPH počas 5-tich rokov pozostávajú z ceny ročnej licencie za 12,3 mil. eur a jednorazovej investície 860 tis. eur na hardvérovú infraštruktúru**. Cena licencie vrátane súvisiacich služieb bola stanovená na základe cenovej ponuky dodávateľa, ktorá sa vzťahuje na 10 organizácií, bez ohľadu na počet aktívnych používateľov. Cena zahŕňa implementáciu a konfiguráciu softvéru, pripojenie vybraných organizácií, poskytovanie technickej podpory a školenie zamestnancov. MV SR zároveň plánuje obstaranie serverového vybavenia kvôli požiadavke na prevádzku riešenia na vlastnej infraštruktúre vládneho cloudu.

Hodnotenie MF SR

- **Zavedenie centrálneho IT nástroja kybernetickej bezpečnosti by malo vychádzať z analýzy rizík, ktorým úrady čelia. Na trhu totiž existujú rôzne riešenia a základom pre výber konkrétneho produktu je poznanie nedostatkov súčasnej ochrany. Zavedenie platformy na báze umelej inteligencie je jednou z možností, ktorá by mala byť porovnaná s inými alternatívami, vrátane posilnenia existujúcich nástrojov (napr. ochrana koncových bodov). Zároveň, obstaranie centralizovaného riešenia pre 10 úradov by malo byť koordinované s NBÚ a MIRRI SR, ktoré majú kybernetickú ochranu štátu tiež v kompetencii.**
    - **Dodatočný prínos zo zavedenia platformy by mala potvrdiť analýza existujúcich rizík.** Podľa zákona o kybernetickej bezpečnosti majú byť bezpečnostné opatrenia prijímané na základe analýzy rizík, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Štúdia neobsahuje konkrétne riziká a údaje o predošlých incidentoch, zraniteľnostiach systému, ani rôznych možnostiach ich predídenia. Bez toho nie je možné objektívne potvrdiť, že navrhovaná platforma je tá najvhodnejšia možnosť na riešenie nedostatkov súčasnej ochrany. Prínosy projektu by mali byť overené a prevýšiť výdavky štátu, ktoré sa zvýšia o 12 mil. eur ročne.
    - **Pri väčšine incidentov môže stačiť ochrana štandardnými nástrojmi spolu s dobre nastavenými procesmi, ktoré je možné dosiahnuť s nižšími finančnými nárokmi.** Podľa Správy o stave kybernetickej bezpečnosti v SR v roku 2024 od NBÚ súvisí najviac incidentov so získavaním informácií pomocou manipulatívnych techník (tzv. phishing), ktoré sú zamerané aj na zamestnancov verejnej správy. Väčšie škody spravidla spôsobujú iné formy útokov (napr. ransomware, malware). Základom ochrany sú štandardné nástroje (zabezpečenie emailov, anti-spoofing, systémy SIEM a EDR) a dobre nastavené procesy (hlásenie, autentifikácia, zmena hesiel, školenia), čo môže stáť rádovo stovky tisíc eur ročne. Pokročilé platformy založené na umelej inteligencii, môžu základnú ochranu rozšíriť o prediktívne schopnosti a umožniť rýchlejšie odhalenie podozrivého správania a znížiť tak reakčný čas pri incidentoch.
    - **Zvýšenú ochranu zo zavedenia novej platformy je preto vhodné overiť v pilotnej prevádzke a až následne ju nasadiť na všetky úrady.** Riešenie vzniklo v roku 2023 a podľa dostupných informácií bolo zatiaľ použité v krajinách Blízkeho východu (Izrael, Spojené arabské emiráty) a v rámci Európy iba v Rakúsku. Produkt zatiaľ nie je bežne využívaný súkromným ani verejným sektorom a informácie o jeho prínose pri zvýšení kybernetickej ochrany nie sú dostupné. Preto je pred jeho plným nasadením vhodné

overiť jeho reálne prínosy v menšom rozsahu, napríklad pilotnou prevádzkou v jednej organizácii, a až následne implementovať na všetky uvažované organizácie.

- **Centralizované riešenie kybernetickej ochrany štátu by malo byť koordinované nadrezortne v spolupráci s NBÚ a MIRRI SR.** Národnú stratégiu, akčný plán aj každoročnú správu o stave kybernetickej bezpečnosti vydáva NBÚ. Zodpovednosť za zabezpečenie kybernetickej ochrany verejnej správy má MIRRI SR, MV SR a MF SR. Tvorbe centralizovaného riešenia pre 10 organizácií by preto mala predchádzať nadrezortná koordinácia a zmapovanie dopadov novej platformy na systémy, procesy a výdavky dotknutých úradov.

- **Z dostupných údajov je primeranosť ceny licencie za 12,3 mil. eur ročne možné overiť len nepriamym porovnaním, nakoľko ide o novú technológiu, ktorá na trhu nemá priamu konkurenciu. Za porovnateľné ceny existujú na trhu aj alternatívne nástroje kybernetickej bezpečnosti, ktoré využívajú AI s podobnými funkcionalitami. Zároveň, presný rozsah potrebného rozširovania IT infraštruktúry za 860 tis. eur nie je z podkladov možné overiť. Podľa informácií MV SR je financovanie projektu plánované zo štátneho rozpočtu.**

  - **Na dodanie navrhovanej platformy má na Slovensku výhradné právo iba jedna firma, čo môže obmedziť priestor pri rokovaniach o konečnej cene.** Na trhu nie sú alternatívni dodávatelia tejto konkrétnej platformy a teda neexistuje motivácia výhradného dodávateľa tlačiť cenu nadol. Nie je tiež známy zdroj financovania nákupu a následnej prevádzky celého projektu.

  - **Okrem preferovaného riešenia existujú na trhu aj alternatívne technológie s čiastočne porovnateľnými funkcionalitami a niektoré z nich sú ponúkané za nižšie jednotkové ceny.** V štúdii bola navrhovaná platforma porovnaná iba s produktom XM Cyber, ktorý MV SR považuje za drahší a technologicky nevyhovujúci. Dodatočne bolo finančné porovnanie rozšírené o ďalšie trhové riešenia, ktoré majú čiastočne porovnateľné funkcionality (Cortex, CrowdStrike, DarkTrace). Napríklad, vo Veľkej Británii sú niektoré z týchto technológií dostupné aj za jednotkové ceny nižšie o 24 % ako je ponuka navrhovanej platformy, resp. o 14 % po zohľadnení požiadavky na nepretržitú podporu. Podľa MV SR však nejde o plnohodnotnú náhradu za preferované riešenie a na pokrytie všetkých požiadaviek by bola potrebná kombinácia technológií, ktorá by sa v konečnom dôsledku prejavila na vyššej cene.

  - **Rozšírenie IT infraštruktúry za 860 tis. eur má vychádzať z požiadavky dodávateľa.** MV SR definovalo požiadavku na umiestnenie technológie priamo vo vlastnom dátovom centre kvôli potrebe spracovania citlivých a utajovaných skutočností. Potreba špecifickej infraštruktúry má byť zároveň podmienkou dodávateľa, na zabezpečenie platnosti záruky a poskytovania zmluvného servisu. Z toho vyplýva potreba rozšírenia súčasnej infraštruktúry o hardvérové komponenty za 860 tis. eur. Potrebu presného počtu nakupovaných zariadení z podkladov nie je možné overiť.

Odporúčania

- Potvrdiť dodatočné prínosy riešenia na základe analýzy rizík a otestovať novú technológiu v pilotnej prevádzke pred jej nasadením na všetky navrhované organizácie.
- Vyhodnotiť, či porovnateľné prínosy nie je možné dosiahnuť aj alternatívnymi nástrojmi s mierne odlišnými funkciami, ktoré môžu byť dostupné za nižšie jednotkové ceny.
- Pri prípadnom centrálnom nasadení technológie zabezpečiť spoluprácu a koordináciu s NBÚ a MIRRI SR a zabezpečiť súlad aj s národnou stratégiou kybernetickej bezpečnosti.

Popis projektu

Ministerstvo vnútra SR (MV SR) plánuje obstarať platformu kybernetickej bezpečnosti založenú na technológii umelej inteligencie (AI). Projekt má byť realizovaný nákupom licencií zvolenej technológie, ktorá využíva modely prediktívnej detekcie kybernetických hrozieb. Navrhovaná investícia má byť podľa štúdie reakciou na čoraz častejšie kybernetické útoky aj konkrétny útok na systémy slovenského katastra nehnuteľností z januára 2025.

Celkové náklady projektu počas piatich rokov majú dosiahnuť 62,4 mil. eur s DPH. Náklady pozostávajú z každoročnej platby za licenciu vo výške 12,3 mil. eur a jednorazovej investície 860 tis. eur na hardvérovú infraštruktúru. Cena licencie vrátane súvisiacich služieb bola stanovená na základe cenovej ponuky dodávateľa, ktorá sa vzťahuje na 10 organizácií, bez ohľadu na počet aktívnych používateľov a počtu zariadení. Cena zahŕňa implementáciu a konfiguráciu softvéru, pripojenie vybraných organizácií, poskytovanie technickej podpory a školenie zamestnancov. MV SR zároveň plánuje obstaranie hardvérového vybavenia kvôli požiadavke na prevádzku riešenia na infraštruktúre vládneho cloudu.

Ciele projektu

Cieľom investície je posilniť odolnosť 10 vybraných organizácií verejnej správy voči kybernetickým hrozbám a zaviesť centralizované riadenie kybernetickej bezpečnosti. Platforma má zabezpečiť jednotný dohľad nad IT infraštruktúrou viacerých organizácií, proaktívne odhaľovanie incidentov a automatizovanú reakciu na prípadné hrozby. Podľa štúdie má projekt naplniť legislatívne požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a európskej smernice o kybernetickej bezpečnosti NIS 2. Podľa MV SR má projekt naplniť legislatívne požiadavky európskej smernice o kybernetickej bezpečnosti NIS 2 a zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, konkrétne v sektore 6.3 Digitálna infraštruktúra a 8.1 Verejná správa.

Identifikácia potreby

Štúdia neobsahuje analýzu rizík súčasnej ochrany, ktorá by mala byť základom pre výber konkrétneho nástroja na zvýšenie kybernetickej bezpečnosti štátu. Návrh konkrétnej kybernetickej ochrany by mal byť založený na detailnej analýze predošlých incidentov a zmapovaní nedostatkov súčasnej ochrany. Aj podľa zákona o kybernetickej bezpečnosti majú byť bezpečnostné opatrenia prijímané na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Predložená štúdia rámcovo pomenúva nedostatky súčasnej ochrany, ako je fragmentácia existujúcich riešení, nedostatočná koordinácia a proaktívna reakcia a preťaženie dátami. Neobsahuje však konkrétne informácie o predošlých incidentoch, identifikovaných zraniteľnostiach, ani rôznych možnostiach ich nápravy. V podmienkach Slovenska sa spomína útok na systémy katastra nehnuteľností, bez konkrétnych údajov o jeho príčine. Bez bližších údajov nie je možné objektívne vyhodnotiť, či je navrhovaná platforma tá najvhodnejšia možnosť na riešenie nedostatkov súčasnej ochrany štátu.

Najviac incidentov na Slovensku súvisí so získavaním informácií prostredníctvom podvodných kampaní, proti ktorým je možné zlepšiť ochranu aj lacnejšími riešeniami. Národný bezpečnostný úrad (NBÚ) vo svojej Správe o stave kybernetickej bezpečnosti v SR v roku 2024 uvádza, že najviac incidentov súvisí so získavaním informácií pomocou manipulatívnych techník (tzv. phishing), ktoré bývajú zamerané aj na zamestnancov verejnej správy. Umelá inteligencia je pri tomto type útokov používaná na tvorbu presvedčivých podvodných kampaní formou personalizovaných správ alebo reklám.

Pri väčšine incidentov môže stačiť ochrana štandardnými nástrojmi spolu s dobre nastavenými procesmi, ktoré je možné dosiahnuť s nižšími finančnými nárokmi. Väčšie škody spravidla spôsobujú iné formy útokov (napr. ransomware, malware). Základom ochrany sú štandardné nástroje (zabezpečenie emailov, anti-spoofing, systémy SIEM a EDR) a dobre nastavené procesy (hlásenie, autentifikácia, zmena hesiel, školenia), čo môže stáť rádovo stovky tisíc eur ročne. Pokročilé platformy založené na umelej inteligencii, môžu základnú ochranu rozšíriť o prediktívne schopnosti a umožniť rýchlejšie odhalenie podozrivého správania a znížiť tak reakčný čas pri incidentoch.

Tvorba centralizovaného riešenia pre 10 organizácií by mala byť koordinovaná v spolupráci s NBÚ a MIRRI SR, ktoré majú kybernetickú bezpečnosť tiež v kompetencii. Národnú stratégiu, akčný plán aj každoročnú správu o stave kybernetickej bezpečnosti vydáva NBÚ. Zodpovednosť za zabezpečenie kybernetickej ochrany verejnej správy má MIRRI SR, MV SR a MF SR. Tvorbe centralizovaného riešenia pre 10 organizácií by preto mala predchádzať nadrezortná koordinácia a zmapovanie dopadov novej platformy na systémy, procesy a výdavky dotknutých úradov.

Analýza alternatív

Štúdia neanalyzuje širšie možnosti zvýšenia kybernetickej ochrany štátu a zvažuje iba možnosť obstarania pokročilých technológií na báze umelej inteligencie. Zvyšovať úroveň kybernetickej ochrany štátu je možné rôznymi spôsobmi, od nastavenia interných procesov (napr. autentifikácia prístupov, školenia zamestnancov), cez štandardne používané nástroje (napr. EDR, SIEM), až po sofistikované technológie na odhaľovanie útokov (napr. platformy na báze AI). Rozhodnutiu o konkrétnom postupe by mala predchádzať analýza rizík, ktorá odhalí zraniteľné miesta a navrhne optimálne riešenie pre jednotlivé typy hrozieb.

Podľa štúdie je navrhovaná platforma výhodnejšia ako alternatívne technológie na trhu. Niektoré riešenia s porovnateľnými funkcionalitami sú pritom ponúkané aj za nižšie jednotkové ceny. V štúdii bola navrhovaná platforma porovnaná iba s produktom XM Cyber, ktorý MV SR nepovažuje za technologicky vhodný, lebo okrem rozdielneho technologického zamerania nie je dostupný ako on-premise riešenie. Dodatočne bolo finančné porovnanie rozšírené o ďalšie trhové riešenia, ktoré majú čiastočne porovnateľné funkcionality (Cortex, CrowdStrike, DarkTrace). Napríklad, vo Veľkej Británii sú niektoré z týchto technológií dostupné aj za jednotkové ceny nižšie o 24 % ako je ponuka navrhovanej platformy, resp. o 14 % po zohľadnení požiadavky na nepretržitú podporu. Podľa MV SR však nejde o plnohodnotnú náhradu za preferované riešenie a na pokrytie všetkých požiadaviek by bola potrebná kombinácia technológií, ktorá by sa prejavila na vyššej celkovej cene.

Ekonomické hodnotenie

Dodatočný prínos zo zavedenia platformy by mala potvrdiť analýza existujúcich rizík. V súčasnosti už sú v štátnych organizáciách zavedené rôzne prvky kybernetickej bezpečnosti, ktoré poskytujú základnú úroveň ochrany proti útokom (napr. firewall, antivírus, nástroje EDR a SIEM). Navrhovaná platforma má byť nadstavbou na tieto nástroje a podľa štúdie má ochranné možnosti štátu ešte rozšíriť. Nové bezpečnostné opatrenia by mali byť prijímané na základe analýzy rizík, ktorá zmapuje konkrétne zraniteľnosti a určí pravdepodobnosť vzniku incidentu. Štúdia neobsahuje konkrétne riziká ani údaje o predošlých incidentoch, dôvodoch ich vzniku, či rôznych možnostiach ich predídenia.

Projekt má zvýšiť šancu pri predchádzaní kybernetickým incidentom, čím má dôjsť k úspore času štátnych zamestnancov v odhadovanej hodnote 23 mil. eur ročne. Dosiahnutie týchto úspor v praxi je však neisté. Riešenie vzniklo len v roku 2023 a podľa dostupných informácií bolo zatiaľ použité v krajinách Blízkeho východu (Izrael, Spojené arabské emiráty) a v rámci Európy iba v Rakúsku. Produkt zatiaľ nie je bežne využívaný súkromným ani verejným sektorom a informácie o jeho prínose pri zvýšení kybernetickej ochrany nie sú dostupné. Dosiahnutie odhadovaných úspor preto nie je možné overiť.

Zvýšenú ochranu zo zavedenia novej platformy je preto vhodné overiť v pilotnej prevádzke a až následne ju nasadiť na všetky zvažované úrady. O účinnosti a prínosoch navrhovanej platformy zatiaľ nie sú dostupné overiteľné údaje keďže ide o novú technológiu, ktorá zatiaľ nie je bežne používaná. Preto je pred jeho plným nasadením vhodné overiť jeho reálne prínosy v menšom rozsahu, napríklad pilotnou prevádzkou v jednej organizácii a až následne pristúpiť k jeho implementácii na všetky uvažované organizácie. MV SR plánuje pred nasadením riešenia na zvažované úrady, otestovať zvolenú technológiu v testovacom prostredí.

Z dostupných údajov nie je možné priamo overiť, či je cena licencie 12,3 mil. eur ročne primeraná, nakoľko ide o novú technológiu, ktorá na trhu nemá priamu konkurenciu. Na dodanie navrhovanej platformy má na Slovensku výhradné právo iba jedna firma, čo môže obmedziť priestor pri rokovaniach o konečnej cene. Financovanie projektu MV SR predpokladá zo zdrojov štátneho rozpočtu.

Potreba rozšírenia IT infraštruktúry za 860 tis. eur má vychádzať z požiadavky dodávateľa. MV SR definovalo požiadavku na umiestnenie technológie priamo vo vlastnom dátovom centre kvôli potrebe spracovania citlivých a utajovaných skutočností. Potreba špecifickej infraštruktúry má byť zároveň podmienkou dodávateľa, na zabezpečenie platnosti záruky a poskytovania zmluvného servisu. Z toho vyplýva potreba rozšírenia súčasnej infraštruktúry o hardvérové komponenty (najmä servery) za 860 tis. eur. Potrebu presného počtu nakupovaných zariadení z podkladov nie je možné overiť.