PODROBNÝ POPIS PROJEKTU

Název projektu	**CZ.31.2.0/0.0/0./24_145/0011561 „Posílení kybernetické bezpečnosti Úřadu městské části Praha 14"**

Manažerský souhrn k obsahu projektu

Projekt „Posílení kybernetické bezpečnosti Úřadu městské části Praha 14" je zaměřen na zvýšení úrovně kybernetické bezpečnosti prostřednictvím komplexního posílení technologických prvků, organizačních opatření a procesů řízení bezpečnosti. Tento projekt zahrnuje oblasti jako správa sítí, datových center, zálohování, monitoring a ochrana aktiv, až po pokročilé nástroje pro identifikaci hrozeb a prevenci útoků.

Projekt reflektuje požadavky relevantních norem a standardů, jako jsou ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework (CSF) a národní legislativa (např. zákon o kybernetické bezpečnosti č. 181/2014 Sb. a související vyhlášky NÚKIB). Implementace těchto opatření přispěje k plnění požadavků směrnice NIS2, která klade důraz na zajištění vysoké úrovně kybernetické bezpečnosti a odolnosti proti kybernetickým hrozbám.

Projekt rovněž přispěje ke snížení investiční náročnosti IT Úřadu městské části Praha 14 v následujících obdobích. Zavedení moderních technologií a optimalizace stávajících systémů umožní efektivnější využití zdrojů a snížení nákladů na údržbu a provoz. Například implementace centralizovaného managementu a monitoringu, automatizace zálohovacích procesů a využití pokročilých bezpečnostních nástrojů povede k dlouhodobým úsporám a zvýšení efektivity.

Klíčové parametry projektu:

- Výzva 46 Kybernetická bezpečnost Národního plánu obnovy Ministerstva vnitra reflektuje potřeby Úřadu městské části Praha 14 na zajištění kybernetické bezpečnosti.
- Uvedená výzva představuje pro MČ Praha 14 příležitost pro zajištění prostředků na zvýšení kybernetické bezpečnosti a souvisejících technologií v rozsahu, který by s ohledem na limitované možnosti bylo obtížné zajistit z vlastních zdrojů.
- Hlavní milníky výzvy:
    - Výzva č. 46 byla vypsána 15. 11. 2024
    - Žádosti byla podána v 02/2025 a nyní probíhá její hodnocení a doplňování

- Rozhodnutí o poskytnutí dotace bylo vydáno 19.6.2025
- Monitorovací indikátory musí být naplněny do 31. 5. 2026
- Nejzazší datum pro fyzické a finanční ukončení realizace projektu: 31. 5. 2026

- Harmonogram a etapizace:
  - Zahájení přípravných činností 23. 7. 2024
  - Zahájení činností na přípravě projektové žádosti 25. 11. 2024
  - Předpokládané schválení projektu RMČ 24. 2. 2025
  - Zahájení činnosti projektového týmu 02/2025
  - Rozhodnutí o poskytnutí dotace bylo vydáno 19.6.2025
  - Zahájení realizace 06/2025
  - Etapa I. podání monitorovací zprávy a žádosti o platbu do 20. 7. 2025 (za období 1. 2. 2025 - 30. 6. 2025)
  - Etapa II. podání monitorovací zprávy a žádosti o platbu do 1.12.2025 (za období 1. 7. 2025 - 30. 11. 2025)
  - Etapa III. podání monitorovací zprávy do 20. 7. 2026 (za období 1. 12. 2025 - 31. 5. 2026)
  - Dodávky služeb a technologií – 08/2025–05/2025
  - Ukončení realizace 31. 5. 2026
  - Ukončení projektu 31. 5. 2026

- Administrace projektu:
  - Administrace projektu ve fázi realizace bude zajištěna na základě VZMR externím subjektem (tato administrace je ve výši 750.000, - Kč uznatelným nákladem projektu).
  - Administrace projektu ve fázi udržitelnosti bude zajištěna interními zdroji Úřadu MČ Praha 14.

- Rozpočet projektu:
  - CELKOVÁ maximální výše dotační žádosti 35.557.825,91 Kč bez DPH
  - DPH v žádosti 6 978 638,73 Kč
  - CELKOVÁ výše dotační žádosti 42 536 464,64 Kč s DPH
  - Hodnota opatření a služeb v projektu 33.131.613,00 Kč bez DPH
    - Opatření již realizovaná a uhrazená z rozpočtu OIKT v předchozích obdobích: 3.554.374,00 Kč bez DPH (tato opatření navyšují celkovou hodnotu projektu,

ale bez dalšího dopadu do již schváleného rozpočtu pro rok 2025, protože již byla uhrazena)

- Opatření, která budou pokryta rozpočtem OIKT na období 02/2025-05/2026 – 1.892.828, - Kč bez DPH (tato opatření navyšují celkovou hodnotu projektu, ale bez dalšího dopadu do již schváleného rozpočtu pro rok 2025, protože jsou zahrnuta v provozních výdajích OIKT na rok 2025)
- Hodnota nově realizovaných opatření v rámci projektu 25.224.411,00 Kč bez DPH.

- Další, plně uznatelné náklady v rámci projektové žádosti:
  - Zpracování projektu projektovou kanceláří a jeho následná administrace – 100.000, - Kč bez DPH
  - Osobní náklady projektu 2.326.212,91 Kč (maximálně 7 % z hodnoty opatření)
- DPH v zákonné výši 6.978.638,73 Kč a náklady na zpracování projektové žádosti ve výši 300.000, - Kč bez DPH nejsou uznatelnými náklady projektu a tyto prostředky představují minimální výši kofinancování MČ Praha 14.
- V rámci Pravidel pro poskytování dotací z rezervy pro MČ HMP na spolufinancování projektů EU/EHP (UF) v rozpočtu hl. m. Prahy bude zažádáno o dotaci na částečné pokrytí podílu na spolufinancování. Jedná se o možné financování 50 % spoluúčasti MČ v tomto případě 3.489.319,37 Kč.
- Udržitelnost projektu:
  - Udržitelnost projektu je stanovena na 5 let.
  - Náklady v době udržitelnosti jsou stanoveny předběžně na základě expertního odhadu obvyklých nákladů s ohledem na skutečnost, že konkrétní technologie nebyly ještě vysoutěženy a vychází z hodnoty nově realizovaných opatření v rámci projektu.
  - Odhadované náklady pro období udržitelnosti ve výši 10 % ročně jsou ve výši 2.522.441,10 Kč bez DPH / rok.

- **Přehled opatření realizovaných v rámci projektu**

ID01 – Pokročilý síťový monitoring	Nástroj pro sběr, analýzu a ukládání síťových toků (netflow), detekci nestandardního síťového provozu a činnosti informačních systémů, jejich uživatelů a administrátorů
ID02 – Posílení primárního datového centra – redundance	Redundantní klastrová řešení Posílení stávajících 3–4 node clusterů tak, aby byla zajištěna vysoká dostupnost a minimalizovány možné výpadky (SPOF). Hyper-V virtualizace. Vytvoření záložních scénářů Připravené procedury pro failover mezi clustery a replikace dat pro zajištění kontinuity služeb.
ID03 – Výměna a implementace aktivních síťových prvků	Implementace moderních switchů. Switche s podporou bezpečnostních funkcí (např. ACL, ochrana proti DDoS na L2/L3 úrovni). Logická mikrosegmentace sítě a IPv6 ready a 802.1X, včetně centralizovaného managementu.
ID04 – Výměna a implementace WiFi infrastruktury	Implementace moderních access pointů. Standard 802.11be (WiFi 7). Nasazení WPA3 a případné nadstavby pro robustnější ochranu. Oddělená SSID a segmentace a centralizovaný monitoring a správa přístupových bodů a kontrolérů.
ID05 – Výměna a implementace zálohovací infrastruktury	Pásková knihovna 2x LTO 9, 40 pozic, včetně příslušenství pro optické připojení. Diskové pole 100TB, optické připojení 2x NAS (redundantní), 100TB, optické připojení 2x server pro zálohování (redundantní) SW: Veškeré licence pro kompletní pokrytí zálohovaného hybridního prostředí na 60 měsíců
ID06 – Zavedení systému řízení kybernetické bezpečnosti včetně sledování a vyhodnocování rizik a atributů na úrovni podpůrných aktiv a výkon role manažera KB	V rámci realizace opatření dojde k vytvoření dokumentace, nastavení procesů a rolí tak, aby byl žadatel plně v souladu s novelizací zákona č. 181/2014 Sb. – implementaci směrnice NIS2. Systém bude implementován do online provozovaného standardního nástroje usnadňujícího následnou správu systému a plnění zákonných povinností včetně plného řízení aktiv a rizik a možnosti automatizovaně a dynamicky definovat případné nové normy formou katalogů hrozeb, zranitelností a opatření. Součástí opatření bude dodavatelské zajištění výkonu role osoby odpovědné za kybernetickou bezpečnost v organizaci žadatele.
ID07 – Firewally pro detašovaná pracoviště	HW: 8 x NGFW pro pracovní skupiny / detašované pracoviště Lokality: (Plechárna, KD Kyje, Gen. Jan., G14, KC Kardašovská, H55, Polyfunkční budova, Správa majetku) SW: Součástí dodávaného FW

ID08 Kompletní správa životního cyklu logů	pro zlepšení sběru, správy a ochrany logů (záznamů událostí) bude implementován pokročilý nástroj pro správu logů (log management). Nástroj bude automaticky sbírat, normalizovat a archivovat logy provozní i bezpečnostní povahy včetně infrastrukturních systémů. Uložené logy budou chráněny proti neoprávněným změnám, a to i v případě archivace. Uložené logy bude možné snadno prohledávat či filtrovat na základě multikriteriálních dotazů napříč zdroji logů. Systém bude obsahovat reportovací a notifikační systém. Notifikace bude možné navázat na výskyt provozní či bezpečnostní nestandardní události.
ID09 Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací	Automatizované vyhledávání známých zranitelností (CVE) ve vnitřních i vnějších systémech. Reportování výsledků Generování přehledů o nalezených slabinách včetně doporučení k nápravě a přiřazení priorit. Integrace s ticketovacím systémem. Soulad s ISO/IEC 27002 (řízení technických zranitelností) a NIST SP 800-40.
ID10 – Konfigurace a implementace bezpečnostních funkcí prostředí Microsoft (Microsoft Entra ID PIM, MFA, AD hardening a zavedení bezpečnostních nástrojů office)	Konfigurace a implementace správy privilegovaných účtů Centralizovaná kontrola uživatelů s rozšířenými oprávněními (administrátoři, servisní účty). Just-In-Time (JIT) přidělování, PAM – privileged access management, hardening Active Directory, pravidelné auditování, kontrola konfigurace, hesel a událostí v AD (logování). Vyšší úroveň ochrany identit, včetně adaptivních bezpečnostních politik. Multi-Factor Authentication (MFA). Plné nasazení a zkušební provoz Microsoft Defender for Office 365, Safe Attachments a Safe Links. Data Loss Prevention (DLP) - nastavení pravidel pro zamezení únikům citlivých informací (např. automatické blokace, šifrování).
ID11 – Zpětné uplatnění – Posílení dostupnosti primárního datového centra a zálohování 2023	Zpětně uplatněné náklady na nákup tří serverů k zajištění HA datového centra, zálohovacího serveru a rozšíření diskového pole z roku 2023
ID12 – Bezpečnostní nástroje Microsoft	Uplatnění perpetuálních licencí Microsoft Business Premium a Microsoft Defender for Business servers zakoupených v roce 2023, 2024 a obnovy licencí v roce 2025.