Dotační programy na kybernetickou bezpečnost ve zdravotnictví

23.2.2023 Kyberbezpečnost pro zdravotnictví – Bratislava

Marek Vaculík, enovation s.r.o.

IROP – výzva č. 5 – Kybernetická bezpečnost (ČR)

Termíny a důležité body

- **Ukončení příjmu žádosti: 27. 7. 2023**
- **Uznatelnost výdajů: 1. 2. 2021 – 1. 12. 2026**
- **Alokace výzvy: 1,6 mld. Kč vyčerpáno cca 55 %**
- **Maximální uznatelné výdaje: 1 – 300 mil. Kč (podle počtu realizovaných opatření)**
- **Míra dotace:**
  - organizační složky státu (100 %)
  - příspěvkové organizace organizačních složek státu (100 %),
  - státní organizace (100 %),
  - státní podniky (64 %),
  - NNO zakládané zde uvedenými typy oprávněných žadatelů (64 %)

IROP – výzva č. 5 – Kybernetická bezpečnost (ČR)

Na co lze podporu využít

Předmětem podpory jsou technická opatření dle Zákona o kybernetické bezpečnosti:

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí; ověřování identity uživatelů; řízení přístupových oprávnění; ochranu před škodlivým kódem; detekci kybernetických bezpečnostních událostí…

Typ nákladů

- Stavební úpravy,
- poplatky za SaaS (po dobu realizace projektu),
- HW a SW,
- penetrační testy,
- Nepřímé výdaje – 7 % z výše uvedených přímých nákladů

NPO – výzva č. 25 – Kybernetická bezpečnost (Praha)

Termíny a důležité body

- Ukončení příjmu žádosti: 30. 4. 2023
- Uznatelnost výdajů: 1. 2. 2020 – 31. 5. 2026
- Alokace výzvy: 774 mil. Kč
- Maximální uznatelné výdaje: 81 mil. Kč / 41 mil. Kč (podle typu zařízení)
- Míra dotace: 100 % (DPH není uznatelným nákladem)
- V rámci projektů hrazených z NPO jsou tedy způsobilé všechny relevantní výdaje přímo spojené s implementací projektu a vynaložené v souvislosti s účelem a výstupy projektu

Národní plán obnovy – nová výzva na kyberbezpečnost

Předpoklad vyhlášení 1/2024

Do 31.3. nutno registrovat záměr na MZd prostřednictvím aplikace Archirepo

Alokace pro zdravotnická zařízení 6 mld. Kč

Předpokládaná výše podpory 100 %

DPH neuznatelným výdajem

enovation

Podporované aktivity

Security audit

Návrh a zavedení systému řízení bezpečnosti informací – procesy a dokumentace

Správa aktiv v oblasti zdravotnické techniky, řízení rizik a zranitelností

Pořízení a implementace nástroje pro zálohování a archivaci

Ochrana integrity komunikačních sítí;

Nástroj pro ověřování identity uživatelů a řízení přístupových oprávnění;

Ochrana před škodlivým kódem;

Nástroj pro detekci, sběr a vyhodnocení kybernetických bezpečnostních událostí;

Servery a disková úložiště, která budou využita v rámci zajištění kybernetické bezpečnosti (virtualizace, ukládání logů aj.).

enovation

Příprava projektové žádosti

Co potřebujeme?

- Bezpečnostní audit – aktuální stav a návrh opatření

Za kolik to pořídíme?

- Stanovení nákladů (rozpočtu projektu) - zajistit cenové nabídky

Jak žádost zpracujeme?

- Studie proveditelnosti – popis aktuálního stavu, popis technických opatření a jejich navázání na ZKB, soulad s realizovanými projekty
- Stanovisko OHA – popis architektury systému

enovation

Typická opatření v žádostech

Zavedení multifaktorové autentizace

Dostupnost a bezpečnost dat – serverovny, disková pole

Síťová bezpečnost – firewall, segmentace

Aktivní síťové prvky

Zvýšení kybernetické odolnosti koncových zařízení implementací pokročilé antivirové ochrany

Systému řízení privilegovaných účtů (PAM)

Pokročilý síťový monitoring, systém centrální správy IP adresního prostoru, odolných základních síťových služeb a řízení přístupu do sítě

Zvýšení ochrany dat a dokumentů společnosti zavedením systému DLP (Data Loss Prevention)

Zvýšení ochrany webových aplikací (WAF f5)

Děkuji za pozornost

Marek Vaculík
✆ +420 776 439 452
marek.vaculik@enovation.cz
www.enovation.cz