|  |  |  |  |
| --- | --- | --- | --- |
| Datum jednání: | 15. 09. 2022 | Bod programu: |  |
| Číslo návrhu: | 318/ZK/22 |
| Název bodu: | Realizace projektu „Zvýšení kybernetické bezpečnosti v Jihočeském kraji I“ a jeho kofinancování, předfinancování způsobilých výdajů a financování nezpůsobilých výdajů z rozpočtu kraje |

|  |  |
| --- | --- |
| Předkladatel: | doc. Ing. Lucie Kozlová, Ph.D. |
| Zpracoval: | OINF |
| **Vedoucí odboru:** | Ing. František Beránek |

NÁVRH USNESENÍ

1. Zastupitelstvo Jihočeského kraje
	1. bere na vědomí
2. 1. žádost odboru informatiky o poskytnutí prostředků z rozpočtu kraje v celkové výši 59 000 000,00 Kč na kofinancování/předfinancování/financování nezpůsobilých výdajů projektu „Zvýšení kybernetické bezpečnosti v Jihočeském kraji I“ a podání žádosti o podporu do 4. výzvy k předkládání žádostí o podporu
z Integrovaného regionálního operačního programu 2021-2027 KYBERNETICKÁ BEZPEČNOST – SC 1.1 (PR), případně do jiné výzvy či jiného dotačního programu; dle přílohy č. 1 návrhu č. 318/ZK/22,
3. 2. další informace uvedené v důvodové zprávě návrhu č. 318/ZK/22;
	1. schvaluje
4. 1. realizaci projektu „Zvýšení kybernetické bezpečnosti v Jihočeském kraji I“ a podání žádosti
o podporu do 4. výzvy k předkládání žádostí o podporu z Integrovaného regionálního operačního programu 2021-2027 KYBERNETICKÁ BEZPEČNOST – SC 1.1 (PR), případně do jiné výzvy či jiného dotačního programu s celkovými výdaji ve výši 59 000 000,00 Kč, z toho způsobilými výdaji projektu ve výši
50 000 000,00 Kč,
5. 2. kofinancování projektu „Zvýšení kybernetické bezpečnosti v Jihočeském kraji I“ z rozpočtu kraje ve výši 7 500 000,00 Kč,
6. 3. předfinancování projektu „Zvýšení kybernetické bezpečnosti v Jihočeském kraji I“ z rozpočtu kraje ve výši 42 500 000,00 Kč,
7. 4. financování nezpůsobilých výdajů projektu „Zvýšení kybernetické bezpečnosti v Jihočeském kraji I“ z rozpočtu kraje ve výši 9 000 000,00 Kč,
8. s čerpáním na základě formuláře evropského projektu dle přílohy č. 1 návrhu č. 318/ZK/22;
	1. ukládá

JUDr. Lukáši Glaserovi, řediteli krajského úřadu, zajistit realizaci usnesení.

DŮVODOVÁ ZPRÁVA

Hlavním cílem projektu je zvýšení kybernetické bezpečnosti a naplnění požadavků daných zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále „ZKB“) a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále „VoKB“), tj. zvýšení bezpečnosti významných informačních systémů (VIS), informačních systémů (IS) a komunikačních systémů (KS) žadatele, a to mimo informační systémy k ochraně utajovaných informací (ISOUI).

V rámci realizace projektového záměru žadatel plánuje realizovat kybernetická bezpečnostní opatření v následujících oblastech dle § 5 odst. 3 zákona č. 181/2014 Sb.:

* b) nástroj pro ochranu integrity komunikačních sítí
* c) nástroj pro ověřování identity uživatelů
* d) nástroj pro řízení přístupových oprávnění
* e) nástroj pro ochranu před škodlivým kódem
* f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů
* h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Všechny VIS, IS a KS žadatele jsou umístěny, provozovány a využívány uživateli v sídlech JČK. V lokalitě na adrese U Zimního stadionu 1952/2, 370 76 České Budějovice je umístěno primární datové centrum JČK a v lokalitě na adrese B. Němcové 49/3, 370 76 České Budějovice je umístěno záložní datové centrum JČK. VIS, IS a KS jsou provozovány z obou datových center JČK v režimu vysoké dostupnosti.

Níže je uvedena návaznost jednotlivých opatření (ID opatření, rozepsána níže) na ZKB a VoKB.

|  |  |  |
| --- | --- | --- |
| ID opatření | ZKB, § 5 odst. 3 zákona | VoKB |
| ID01Rozšíření stávající platformy Log Management a SIEM | f) a h) | § 22 odst.1 písm. a), § 22 odst. 2 písm. b), c), d)§ 22 odst. 4§ 24 písm. a) až f) |
| ID02Rozšíření systému pro správu privilegovaných účtů o identity management a správu externích uživatelů | d) | § 20 písm. a) a b) |
| ID03Modernizace ochrany komunikační sítě perimetrovými firewally | b) | § 18 písm. a) až e) |
| ID04Implementace technologie pro řízení přístupu ke komunikační síti | c) | § 19 odst. 1§ 19 odst. 2 písm. a) až g)§ 19 odst. 4 |
| ID05Implementace ochrany proti útoku typu ransomware | e) | § 21 odst. 1 písm. a) a e)§ 21 odst. 2 |

Souhrnně je účelem projektu realizace technických bezpečnostních opatření podle § 5 odst. 3 ZKB v souladu s výzvou č. 4 IROP 2021-2027.

Cílem projektu je zajištění technických bezpečnostních opatření dle ZKB k zajištění bezpečnosti systémů žadatele před kybernetickými útoky, nežádoucími aktivitami a monitoring těchto systémů.

**Obsah projektu, realizovaná opatření**

Výpis projektem zabezpečovaných VIS/IS/KS.

**Významné informační a komunikační systémy**

Informační a komunikační systémy JČK, klasifikované jako Významné informační systémy podle § 3 odst. 2 vyhlášky č. 317/2014 Sb.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Označení IS/KS | Výkon působnostipodporovaný systémem  | VIS | Naplněné kritérium | VIS ID | KS ID |
| Ekonomický informační systém (IS GINIS EKO) | Zajištění plateb | ANO | § 3 odst. 1 písm. b) | 1 |  |
| MS Exchange Server | Komunikace a zajištění podání | ANO | § 2 odst. 1 písm. a) | 2 | 1 |
| Oficiální www stránky Jihočeského kraje (Elektronická úřední deska je součástí www stránek JK) | Zajištění informování veřejnosti orgánem veřejné moci | ANO | § 3 odst. 1 písm. e) | 3 | 2 |
| Spisová služba (IS GINIS modul SSL)  | Vedení správních řízení, spisová služba | ANO | § 2 odst. 1 písm. d)§ 3 odst. 1 písm. c) | 4 |  |

**Informační systémy**

Informační systémy JČK, které nejsou klasifikované jako Významné informační systémy podle § 3 odst. 2 vyhlášky č. 317/2014 Sb., nicméně budou také zabezpečovány pomocí bezpečnostních opatření v rámci projektu.

|  |  |  |
| --- | --- | --- |
| Označení IS | Výkon působnostipodporovaný systémem  | IS ID |
| ANET - TIME verze 10.xx | Docházkový systém | 1 |
| Cestovní příkaz | Evidence cestovních příkazů | 2 |
| ESPI - Evidence správních řízení, EVI - Evidence odpadů, zařízení | Evidence | 3 |
| eSPIS Lite | Spisová služba pro externí subjekty | 4 |
| Evidence dopravních agend | Evidence | 5 |
| Evidence majetku (WinEMA - majetek PO) | Evidence | 6 |
| Evidence myslivosti | Evidence | 7 |
| Evidence středních a malých zdrojů (OvzdusiSQL) | Evidence | 8 |
| FLUXPAM verze 5 | Personální a mzdový systém | 9 |
| Geoportál JčK | Rozcestník pro různé veřejné služby GIS | 10 |
| IDM | Systém pro správu identit | 11 |
| Intranet | Interní IS | 12 |
| IS GINIS - zbývající moduly | Výkon působnosti v rozsahu jednotlivých modulů | 13 |
| iUSNESENI | Zajištění zpřístupnění materiálů do rady JK | 14 |
| Neveřejné stránky pro zřizované organizace | Podpora zřizovaných organizací | 15 |
| Personalistika | Personální systém | 16 |
| Stavební úřad | Systém pro podporu stavebních agend | 17 |
| Twist | Systém pro nahlížení dat do katastru nemovitostí | 18 |
| Účetnictví a rozpočet (GorUCR) | Správa rozpočtů zřizovaných organizací | 19 |
| Výkaznictví (GorVYK) | Správa výkazů zřizovaných organizací | 20 |

**Komunikační systémy**

Komunikační systémy JČK, které nejsou klasifikované jako Významné informační systémy podle § 3 odst. 2 vyhlášky č. 317/2014 Sb., nicméně budou také zabezpečovány pomocí bezpečnostních opatření v rámci projektu.

Dále jsou uvedena jednotlivá opatření a jejich stručný popis:

|  |  |
| --- | --- |
| ID opatření: | 01  |
| Oblast opatření podle ZKB a VoKB: | Oblast opatření podle ZKB:f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorůh) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostíOblast opatření podle VoKB:§ 22 odst.1 písm. a), odst. 2 písm. b), c), d), odst. 4§ 24 písm. a) až f)  |
| Název opatření: | Rozšíření stávající platformy Log Management a SIEM |
| KII/VIS/ISZS/IS/KS: | Opatření se týká všech VIS žadatele, tj. VIS ID 1 až 4Opatření se týká všech IS žadatele, tj. IS ID 1 až 20Opatření se týká KS žadatele, tj. KS ID 1 |
| Popis opatření: | Změna architektury a rozšíření stávajícího systému ArcSight pro logování (log management) a vyhodnocování bezpečnostních událostí (SIEM). Bude vyprojektována nová architektura dotčených systémů včetně architektury dotčené běhové infrastruktury, následně bude provedeno doplnění infrastruktury o potřebné výpočetní a úložné kapacity, nákup nových rozšiřujících licencí software pro log management a SIEM a implementace řešení.Nově implementované řešení bude rozšiřovat stávající tak, aby bylo možné efektivně napojit do systému sběr logů z dalších implementovaných opatření, dalších IS, infrastruktury a jiných systémů žadatele, které doposud aktuálně využívaný systém LM a SIEM nesbírá a nevyhodnocuje. Tyto informace dále analyzovat a vyhodnocovat pro zajištění minimalizace bezpečnostních rizik. |
| Sdílení opatření se ISOUI: | - |

|  |  |
| --- | --- |
| ID opatření: | 02 |
| Oblast opatření podle ZKB a VoKB: | Oblast opatření podle ZKB:d) nástroj pro řízení přístupových oprávněníOblast opatření podle VoKB:§ 20 písm. a) a b) |
| Název opatření: | Rozšíření systému pro správu privilegovaných účtů o identity management a správu externích uživatelů |
| KII/VIS/ISZS/IS/KS: | Opatření se týká všech VIS žadatele, tj. VIS ID 1 až 4Opatření se týká všech IS žadatele, tj. IS ID 1 až 20Opatření se týká KS žadatele, tj. KS ID 1 |
| Popis opatření: | Nástroj pro kontrolu operací privilegovaných uživatelů bude rozšířen na širší okruh uživatelů, zahrnující nově externí uživatele pro zajištění vyšší úrovně bezpečnosti a kontroly nad privilegovanými přístupy. Bude provedeno rozšíření stávajícího řešení správy privilegovaných účtů od výrobce CyberArk. Cílem rozšíření řešení je pokrytí nástroje pro externích 30 uživatelů.Součástí opatření je také zajištění navýšení robustnosti stávajícího řešení tak, aby výpadek jedné komponenty nezpůsobil nedostupnost řešení (eliminace SPoF) |
| Sdílení opatření se ISOUI: | - |

|  |  |
| --- | --- |
| ID opatření: | 03 |
| Oblast opatření podle ZKB a VoKB: | Oblast opatření podle ZKB:b) nástroj pro ochranu integrity komunikačních sítíOblast opatření podle VoKB:§ 18 písm. a) až e) |
| Název opatření: | Modernizace ochrany komunikační sítě perimetrovými firewally |
| KII/VIS/ISZS/IS/KS: | Opatření se týká všech VIS žadatele, tj. VIS ID 1 až 4Opatření se týká všech IS žadatele, tj. IS ID 1 až 20Opatření se týká KS žadatele, tj. KS ID 1 |
| Popis opatření: | Do každého z datových center bude pro snížení hrozeb z pohledu kybernetické bezpečnosti a také pro zajištění požadovaného výkonu a propustnosti implementován perimetrový firewall, kterým bude provedena zásadní bezpečnostní a výkonová modernizace stávajícího, bezpečnostně i výkonově nevyhovujícího zařízení. Perimetrový firewall bude zajišťovat pokročilou inspekci provozu na L7 vrstvě, bude sloužit jako VPN koncentrátor, bude zajišťovat Threat ochranu, Malware ochranu a URL filtraci. Pro oba firewally bude implementován centralizovaný nástroj pro jejich správu, instalovaný do VMware virtualizačního prostředí žadatele. |
| Sdílení opatření se ISOUI: | - |

|  |  |
| --- | --- |
| ID opatření: | 04 |
| Oblast opatření podle ZKB a VoKB: | Oblast opatření podle ZKB:c) nástroj pro ověřování identity uživatelů;Oblast opatření podle VoKB:§ 19 odst. 1§ 19 odst. 2 písm. a) až g)§ 19 odst. 4 |
| Název opatření: | Implementace technologie pro řízení přístupu ke komunikační síti |
| KII/VIS/ISZS/IS/KS: | Opatření se týká všech VIS žadatele, tj. VIS ID 1 až 4Opatření se týká všech IS žadatele, tj. IS ID 1 až 20Opatření se týká KS žadatele, tj. KS ID 1 |
| Popis opatření: | Bude nasazena technologie řízení přístupu k interní síti LAN, která zabrání připojení neautorizovaných uživatelů a zařízení do interní sítě JČK. Veškerá zařízení, která budou jakoukoli formou (wired či wireless) připojena do sítě JČK, budou muset být autentizována a autorizována, v opačném případě nebudou systémem vpuštěna do sítě a k jejím zdrojům jako jsou VIS, IS a KS. |
| Sdílení opatření se ISOUI: | - |

|  |  |
| --- | --- |
| ID opatření: | 05 |
| Oblast opatření podle ZKB a VoKB: | Oblast opatření podle ZKB:e) nástroj pro ochranu před škodlivým kódemOblast opatření podle VoKB:§ 21 odst. 1 písm. a) a e)§ 21 odst. 2 |
| Název opatření: | Implementace ochrany proti útoku typu ransomware |
| KII/VIS/ISZS/IS/KS: | Opatření se týká všech VIS žadatele, tj. VIS ID 1 až 4Opatření se týká všech IS žadatele, tj. IS ID 1 až 20 |
| Popis opatření: | Rozšíření stávajícího zálohovacího systému o systém ochrany proti napadení útokem typu ransomware. Bude provedena implementační analýza, pořízení hardware pro ukládání zálohovaných dat VIS, IS a KS JČK do odděleného offline prostředí od záloh stávajících, pořízení software pro správu odděleného zálohovacího prostředí a pro kontrolu konzistence záloh za účelem včasné detekce možného napadení zálohovaných dat. |
| Sdílení opatření se ISOUI: | - |

Rozpočet projektu byl stanoven na základě průzkumu trhu zohledněného o inflaci. Servisní podpory, služby, maintenance představují dle průzkumu trhu částku cca 29,6 mil. Kč za pět let.

**Celkové výdaje projektu včetně 5 let servisní podpory představují částku 88 600 000,00 Kč:**

**Způsobilé výdaje: 50 000 000,00 Kč**

**Nezpůsobilé výdaje: 9 000 000,00 Kč**

**Servisní podpory, služby, maintenance: 29 600 000,00 Kč**

Tento materiál projednala rada kraje na svém jednání 1. 9. 2022 a usnesením č. 953/2022/RK-49doporučila zastupitelstvu realizaci projektu schválit

Finanční nároky a krytí: Projekt je zahrnut v tabulce „Přehled investičních akcí 2022 - 2027 (včetně transferů PO)“ a bude součástí návrhu rozpočtu na rok 2023.

Vyjádření správce rozpočtu: Ing. Michaela Zárubová (OEKO): Souhlasím, prostředky by měly být zahrnuty do návrhu rozpočtu na rok 2023 a zároveň aktualizovány částky v tabulce „Přehled investičních akcí 2022 - 2027 (včetně transferů PO)“.

Návrh projednán (stanoviska): není požadováno

PŘÍLOHY:

1. Formulář evropského projektu „Zvýšení kybernetické bezpečnosti v Jihočeském kraji I“ (Formular\_evropskeho\_projektu\_IROP - kybernetická bezpečnost I final.xlsx)

Zodpovídá: pověřený vedoucí OINF – Ing. František Beránek

Termín kontroly: 31. 12. 2022

Termín splnění: 28. 2. 2024