Nová investice „Kybernetická bezpečnost II“

1. Popis komponenty

|  |
| --- |
| **Nová investice - „Kybernetická bezpečnost II“**  **Oblast politiky:** *eGovernment, digitalizace veřejné správy*  **Komponenta: 1.2 – Digital public administration systems**  **Cíl:**  Cílem je posílení kybernetické bezpečnosti subjektů působících v oblasti dopravy, IZS, veřejné správy a zdravotnictví.  **Reformy a investice:**  **Investice**  Nová investice „Kybernetická bezpečnost II“  Cílem investice je další posílení investice do kybernetické bezpečnosti v rámci nenávratné finanční podpory navýšením počtu informačních systémů, jejichž kybernetická bezpečnost byla posílena v souladu se zákonem č. 181/2014 Sb. na 244 veřejných informačních systémů.  **Odhadované náklady:**  6,6 mld. Kč (plně zahrnuto do RRF) |

2. Hlavní výzvy a cíle

1. Hlavní výzvy

S ohledem na aktuální situaci, značně ovlivněnou ruskou agresí na Ukrajinu a s tím přidružených okolností, je vhodné přidat novou investici „Kybernetická bezpečnost II“ do komponenty 1.2 stávajícího Národního plánu obnovy.

Konkrétní důvody pro přidání nové investice:

1. **Kybernetické útoky na Českou republiku**
2. Dle Výroční zprávy NUKIB (Národní úřad pro kybernetickou a informační bezpečnost[[1]](#footnote-2)) – Zprávy o stavu kybernetické bezpečnosti České republika za rok 2021 – došlo v roce 2021 oproti roku 2020 k cca 50% nárůstu v počtu bezpečnostních incidentů.
3. Pravidelný měsíční materiál „Kybernetické incidenty pohledem NÚKIB“ ukazuje klasifikaci incidentů a nejčastější cíle kybernetických útoků. Data z ledna 2023[[2]](#footnote-3) ukazují dvojnásobný nárůst kybernetických útoků oproti minulému měsíci, meziročně se jedná také o dvojnásobný nárůst. I nadále zůstávají hlavními útočníky hackerské skupiny z Ruska. V absolutních číslech se jedná o desítky kybernetických útoků měsíčně.
4. Oblast veřejné správy je nejčastěji zasaženým sektorem, přičemž během větších útočných kampaní (např. DDoS útoky ruskojazyčné skupiny Killnet) je vždy mezi hlavními napadenými. V minulosti byly evidovány významné incidenty, kdy se subjekty veřejné správy staly terčem kyber-špionáže nebo ransomwaru, přičemž se jednalo jak o celostátní organizace, tak o ty působící na lokální úrovni (např. samosprávy).

Mezi další hlavní cíle útoku patří subjekty z oblasti dopravy. Oblast dopravy se stala významným terčem v roce 2022, kdy došlo nad rámec kybernetických útoků, technických zranitelností a chyb, k několika DDoS útokům proti letištím. V kontextu ruské agrese proti Ukrajině se pravděpodobnost kybernetického útoku na dopravní infrastrukturu navyšuje, a to vzhledem ke skutečnosti logistického významu ČR v době případného válečného konfliktu. Zdravotnictví - je často terčem útoků s důsledkem velmi významných incidentů (např. ransomware). Přestože pominula největší zátěž, jež na zdravotnictví směřovala během pandemie covid-19, tak úspěšný kybernetický útok může mít dalekosáhlé dopady. Ty se mohou projevit v zašifrování systémů a navazující nemožnosti poskytovat lékařskou péči. I přes již realizované investice do kybernetické bezpečnosti prostřednictvím nemocnic v Praze (které jsou vyjmuty z možnosti financování kybernetických opatření prostřednictvím kohezních fondů) se jedná o oblast s velkým deficitem financování. Oblast zdravotnictví rovněž disponuje v rámci veřejných služeb největším objemem zvláštních kategorií osobních údajů, jejichž kompromitace může významně poškodit zdravotnické zařízení i pacienty.

1. **Implementace směrnice NIS2**
2. V průběhu následujících let musí ČR transponovat a také implementovat požadavky směrnice NIS2, která přináší mnoho změn v oblasti zajišťování kybernetické bezpečnosti a týká se nejen organizací, které jsou již dnes ze zákona o kybernetické bezpečnosti povinny své systémy zabezpečovat, ale i velkého množství organizací, které budou do regulace spadat nově a do dnešního dne žádné povinnosti plnit nemusely. Nově tak bude požadavkům a změnám specifikovaným ve směrnici NIS2 podléhat více než 6000 subjektů v ČR namísto nynějších několika málo stovek.
3. **Vysoká poptávka po finančních zdrojích**
4. Vedle investice „Kybernetická bezpečnost“ v Národním plánu obnovy je k dispozici i další finanční zdroj – konkrétně Integrovaný regionální operační program+ (IROP+), který je v gesci Ministerstva pro místní rozvoj. IROP+ vyhlásil celkem 3 výzvy na zajištění kybernetické bezpečnosti, přičemž 2 z nich mají převis poptávky po finančních zdrojích oproti disponibilním prostředkům ve výši 3 mld. Kč[[3]](#footnote-4) Existuje zde tedy značná potřeba finančního posílení dané oblasti.
5. Cíle

Hlavním cílem je zvýšit úroveň kybernetické bezpečnosti u vybraných centrálních úřadů, institucí, a subjektů v oblasti dopravy dle zákona o kybernetické bezpečnosti a souvisejících předpisů. Primárním cílem bude

* podpora subjektů z oblasti dopravy spadající pod směrnici NIS2, a to z důvodu navýšené četnosti kyberútoků do této oblasti v posledních měsících
* podpora subjektů z oblasti zdravotnictví, a to subjekty spadající pod kategorii „essential“ dle směrnice NIS2 a ve vybraných případech rovněž „essentials“
* podpora dalších subjektů z oblasti veřejné správy

Předpokládá se poskytnutí podpory pro několik stovek subjektů, z toho primárně z oblasti dopravy a oblasti veřejné správy. Průměrná výše finanční podpory na projekt je odhadována na 30 mil. Kč (uvedená hodnota odpovídá průměrné výši žádosti o finanční podporu v rámci Integrovaného regionálního operačního programu).

Navýšení kybernetické bezpečnosti bude provedeno realizací následujících činností:

* analýzy rizik
* implementací bezpečnostních opatření vzešlých z analýzy rizik
* provedením auditu kybernetické bezpečnosti potvrzující soulad s legislativou

Podporovanými aktivitami budou například:

* Zajištění služeb auditu kybernetické bezpečnosti včetně penetračních či jiných bezpečnostních testů
* Návrh a zavedení systému řízení bezpečnosti informací a báze znalostí v oblasti kybernetické bezpečnosti včetně souvisejících procesů a dokumentace
* Pořízení a implementace nástroje pro zálohování a archivaci
* Zabezpečení komunikační sítě v rozsahu L2/L3 switche a nástroje pro segmentaci datové komunikační sítě, NAC, 802.1X
* Pořízení a implementace NGFW vč. IPS/IDS
* Pořízení a implementace Endpoint protection řešení
* Pořízení a implementace nástroje pro load balancing
* Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu
* Pořízení a implementace nástroje pro multifaktorovou autentizaci
* Pořízení a implementace nástroje pro log management
* Pořízení a implementace nástroje pro SandBoxing
* Dodávka a implementace SIEM, služby SOC
* Dodávka a implementace nástroje z kategorie Advanced Threat Protection
* Dodávka a implementace nástroje pro řízení přístupů a identit (PIM/PAM, atp.)
* Pořízení a implementace nástroje pro Mobile/Enterprise device management
* Pořízení a implementace nástroje pro správu aktiv a řízení rizik a zranitelností
* Servery a disková úložiště, která budou přímo využita v rámci zajištění kybernetické bezpečnosti (virtualizace, ukládání logů aj.)
* Pořízení kryptografického systému zajišťující ochranu informací mezi datovými centry a uživatelskými pracovními stanicemi přenášených po nezabezpečeném komunikačním prostředí různých poskytovatelů a současně zajistí kybernetickou bezpečnost provozovaných aplikací.
* Další dle objektivní potřeby

1. Národní strategický kontext

Zajištění kybernetické bezpečnosti vychází z:

* Národní strategie kybernetické bezpečnosti na období 2021 – 2025[[4]](#footnote-5)

1. Předchozí snahy

Financování oblasti kybernetické bezpečnosti je podporováno na několika úrovních:

1. Integrovaný regionální operační program – období 2014 – 2020 – celková alokace 1,1 mld. Kč
2. Integrovaný regionální operační program - období 2021 – 2027 – celková alokace 3,3 mld. Kč
3. Národní plán obnovy – investice „Kybernetická bezpečnost“ – celková alokace 2,7 mld. Kč

V návaznosti na aktuální finanční hodnoty podaných projektových žádostí v IROP oproti disponibilním finančním prostředkům IROP (až 300%)[[5]](#footnote-6) je viditelná vysoká poptávka po posílení kybernetické bezpečnosti.

3. Popis reforem a investic komponenty

1. Popis reforem

*Není relevantní, podpora zahrnuje pouze investiční opatření*

1. Popis investic

|  |  |
| --- | --- |
| Výzva | *Zajištění kybernetické bezpečnosti* |
| Cíl | Zvýšit úroveň kybernetické bezpečnosti u centrálních úřadů, institucí a dalších subjektů dle zákona o kybernetické bezpečnosti a souvisejících předpisů. |
| Implementace | *Ministerstvo vnitra, příjemci z řad subjektů veřejné správy (doprava, IZS, zdravotnictví a ostatní)* |
| Spolupráce a zapojení zúčastněných stran | *Ministerstvo vnitra, Ministerstvo zdravotnictví, Ministerstvo dopravy* |
| Překážky a rizika | ***Zpoždění v přípravě jednotlivých zadávacích dokumentací***   * *Z dosavadních aktivit podpory kybernetické bezpečnosti existují na straně příjemců již značně připravené projektové dokumentace v rámci programů IROP.* * *Pro eliminaci rizika budou při hrozícím zpoždění v přípravě zadávacích dokumentací využity eskalační procedury a následně využity personální kapacity Digitální informační agentury, případně dalších subjektů a příp. dalších kompetenčních center v závislosti na potřebných odbornostech.*   ***Zahlcení OHA při vydávání stanovisek a s tím související delší vydávání souhlasných stanovisek***   * *Pro eliminaci rizika budou při hrozícím zpoždění v přípravě vydávání stanovisek OHA budou využity eskalační procedury na Digitální informační agenturu a Radu vlády pro informační společnost s požadavkem na doplnění kapacit OHA.*   ***Nekvalitní architektonické návrhy, které si vyžádají opakované projednávání***   * *Pro eliminaci rizika budou využívány konzultace architektonických návrhů s pracovníky kompetenčních center*   ***Posun v realizaci zadávacích řízení vč. rozhodování ÚOHS***   * *Riziko je nutné akceptovat.*   ***Zpoždění v implementaci jednotlivých systémů a služeb****.*   * *K eliminaci rizika slouží vícestupňový dohled nad realizací jednotlivých projektů a současně personální kapacity příjemců, příp. dalších kompetenčních center, která budou moci poskytnout specialisty pro řešení situace.* |
| Cílové skupiny populace a ekonomické subjekty | *Primární cílovou skupinou jsou hlavní nositelé projektů, neboť se jedná především o systémy zaměřené na digitalizaci vnitřního chodu úřadu, příp. výkonu agend vykonávaných v rámci přenesené působnosti.*  Sekundární cílovou skupinou je široká veřejnost využívající služby hlavních nositelů projektů.  Realizace nových projektů bude probíhat prostřednictvím otevřených výzev, případně předem definovaných projektů směřujících do oblastí veřejné správy, IZS, zdravotnictví a dopravy. Disponibilní finanční alokace, pokud nebude k dispozici celá částka 6,6 mld. Kč, bude rozdělena poměrově s důrazem na oblast veřejné správy, přičemž poměr se může měnit na základě aktuální potřeby v oblasti kybernetických hrozeb. |
| Souhrnné náklady realizace financované z RRF za celé období | *6,6 mld. Kč* |
| Dodržování pravidel státní podpory | *Investice nezakládá veřejnou podporu.*  Pro vyloučení možnosti vzniku dvojího financování se uplatňuje pravidlo, kdy úspěšný žadatel o finanční podporu v rámci IROP + nemůže současně žádat o finanční podporu v rámci výzev NPO.  Jednotlivé projekty budou realizovány v souladu s pravidly pro zadávání veřejných zakázek (otevřená výběrová řízení) a zásadami řádného finančního řízení. Tím bude zajištěno, že stát bude za pořizované služby platit tržní ceny, nebude tedy poskytnuta žádná státní podpora. Zároveň realizace projektů přispívá k bezpečnému výkonu veřejné moci. Státní podporu lze tedy považovat za vyloučenou dle GT A/a/13. |
| Uveďte dobu implementace | *Q3 2023 – Q4 2025* |

4. Strategická autonomie a bezpečnostní problematika

Komponenta jako celek je zcela v souladu s aktuálními opatřeními a trendy v oblasti kybernetické bezpečnosti a mnohé z nich rozvíjí a implementuje. Vychází ze strategií:

* Národní strategie kybernetické bezpečnosti na období 2021 – 2025

5. Přeshraniční a mezinárodní projekty

Investice se týká zajištění podmínek pro umožnění přeshraniční spolupráce.

6. Zelený rozměr komponenty

Není relevantní

7. Digitální rozměr komponenty

Jedná se o investici se 100% digital „tagging“.

8. Uplatnění zásady „významně nepoškozovat“

Veškeré investice vzhledem ke svému charakteru princip „významně nepoškozovat“ naplňují.

9. Milníky, cíle a harmonogram

Jako konečný cíl podpory byl zvolen model aktualizace milníků a cílů ve stávající investici „Kybernetická bezpečnost“, konkrétně:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| New Investment:  **Top-up of cyber security investment** | Milestone | Publication of the call relating to the strengthening of information systems according to Act No. 181/2014 Coll., on cyber secirity | Publication of a call for projects |  |  | Q1 | 2024 | Publication of a call for projects supporting the strengthening of information systems according Act No. 181/2014 Coll., on cyber security. |
| New Investment:  **Top-up of cyber security investment** | Target | Information systems whose cyber security has been strengthened in line with Act No. 181/2014 Coll., on cyber security | Number | 87 | 331 | Q4 | 2025 | The target shall increase the cybersecurity of the selected information systems in accordance with the requirements of Act No. 181/2014 Coll., on cyber security.  The target shall be considered as achieved following the successful testing and verification of compliance with cyber security requirements of at least 244 information systems. The authorities in charge of the information systems shall approve the delivery of the respective systems |

Očekává se několik stovek projektů v oblasti kybernetické bezpečnosti, a to napříč subjekty veřejné správy.

(zákon 181/2014 Sb. o kybernetické bezpečnosti, 134/2016 Sb. o zadávání veřejných zakázek a relevantních vyhlášek).

Předpokládá se, že v roce 2023 dojde k přípravě a zveřejnění výzev, podání žádostí o finanční podporu a zahájení veřejných zakázek. V roce 2024 očekáváme zahájení prvních realizací.

**Očekávaná hodnota cíle**

Každý subjekt spravuje určitý počet informačních systémů (jiný je počet u institucí v oblasti dopravy či na území samospráv). Uspokojivým výsledkem je zajištění kybernetické bezpečnosti u 244 informačních systémů.

**Termín dosažení cíle**

31. 12. 2025

**Odpovědná instituce**

Ministerstvo vnitra

**Harmonogram**

Předpokládá se, že po schválení tohoto rozšíření investice („update NPO“) v roce 2023 dojde do několik málo měsíců k vypsání výzev, které budou soutěžní a rovněž pro předem definované projety (např. na Ministerstvu vnitra dojde k výběru předem definovaných projektů na základě závěrů Komise pro koordinaci projektů kybernetické bezpečnosti v resortu Ministerstva vnitra)  Následně dojde k podání žádostí o finanční podporu a zahájení veřejných zakázek. V roce 2024 očekáváme start prvních realizací. Předpoklad je, že do 4Q 2025 bude 244 informačních systémů zabezpečeno v souladu s požadavky směrnice NIS2, respektive zákona 181/2014Sb. o zajištění kybernetické bezpečnosti (který směrnici NIS2 transponuje do české legislativy.

10. Financování a costing

**Srovnávací údaje o nákladech**

*Vycházíme z*

* *dat z žádostí o finanční podporu u projektových žádostí v Integrovaném regionálním operačních programu*+  *- cca 27 mil. Kč na 1 projekt v oblasti kybernetické bezpečnosti*

|  |  |
| --- | --- |
| **IROP+ výzvy 3 a 4 – stav k únoru 23** | **Celkem** |
| Celkem podaných žádostí o podporu | 244 |
| Celková výše požadovaného příspěvku | 6 572 631 468,31 Kč |
| **Průměrná výše požadovaného příspěvku** | **26 937 014,21 Kč** |

* *výsledků průzkumu absorpční kapacity mezi subjekty z oblasti zdravotnictví a dopravy*
* *převisu poptávky po finančních zdrojích v rámci výzev IROP+ (očištěno o subjekty z oblasti zdravotnictví a dopravy)*
  + *celkem podáno několik desítek projektů v hodnotě 1,69 mld. Kč*

**měnit v návaznosti s ohledem na aktuální kybernetické hrozby)**

|  |  |  |  |
| --- | --- | --- | --- |
|  | předpokládaný počet podpořených projektů | průměrná výše finanční podpory na žádost (mil. Kč) | celková absorpční kapacita v mil. Kč |
| Doprava, veřejná správa, zdravotnictví | 244 | 27 | 6600 |

Z dat IROP+ vyplývá, že v rámci jednoho projektu, který byl podán do výzev č. 3 a 4 je posílen minimálně jeden informační systém dle principů kybernetické bezpečnosti.

11. Další EU zdroje financování

Vedle zde řešené investice „K kybernetická bezpečnost“ v Národním plánu obnovy je k dispozici i další finanční zdroj – konkrétně Integrovaný regionální operační program (IROP), který je v gesci Ministerstva pro místní rozvoj. IROP vyhlásil celkem 3 výzvy na zajištění kybernetické bezpečnosti, přičemž 2 z nich mají převis poptávky po finančních zdrojích oproti disponibilním prostředkům ve výši 3 mld. Kč[[6]](#footnote-7)

Jednou z podmínek finanční podpory projektu z prostředků NPO je nečerpání finanční podpory z IROP z uvedených výzev. Jinými slovy, subjekt, který byl úspěšný v rámci výzev IROP+, nemůže současně podávat žádost do výzev NPO.

**Financování půjčkami:**

Pokrytí dodatečného financování půjčkami se předpokládá.

1. [Národní úřad pro kybernetickou a informační bezpečnost - Zprávy o stavu KB (nukib.cz)](https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/) [↑](#footnote-ref-2)
2. [Národní úřad pro kybernetickou a informační bezpečnost - Kybernetické incidenty pohledem NÚKIB - leden 2023 (nukib.cz)](https://www.nukib.cz/cs/infoservis/aktuality/1934-kyberneticke-incidenty-pohledem-nukib-leden-2023/) [↑](#footnote-ref-3)
3. [IROP - Ministerstvo pro místní rozvoj ČR - Seznam projektů ve 3. a 4. výzvě Kybernetická bezpečnost IROP ve stavu hodnocení k 1. 2. 2023 (mmr.cz)](https://irop.mmr.cz/cs/ostatni/web/novinky/seznam-projektu-3-a-4-vyzva-stav-hodnoceni) [↑](#footnote-ref-4)
4. [Národní úřad pro kybernetickou a informační bezpečnost - Strategie / Akční plán (nukib.cz)](https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/) [↑](#footnote-ref-5)
5. [IROP - Ministerstvo pro místní rozvoj ČR - Seznam projektů ve 3. a 4. výzvě Kybernetická bezpečnost IROP ve stavu hodnocení k 1. 2. 2023 (mmr.cz)](https://irop.mmr.cz/cs/ostatni/web/novinky/seznam-projektu-3-a-4-vyzva-stav-hodnoceni) [↑](#footnote-ref-6)
6. [IROP - Ministerstvo pro místní rozvoj ČR - Seznam projektů ve 3. a 4. výzvě Kybernetická bezpečnost IROP ve stavu hodnocení k 1. 2. 2023 (mmr.cz)](https://irop.mmr.cz/cs/ostatni/web/novinky/seznam-projektu-3-a-4-vyzva-stav-hodnoceni) [↑](#footnote-ref-7)