MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Vybrané projekty zamerané na rozvoj informačnej a kybernetickej bezpečnosti vo verejnej správe

Mgr. Filip Tubler
Odbor riadenia kybernetickej a informačnej bezpečnosti
Sekcia kybernetickej bezpečnosti

06.10.2022

Informačná a kybernetická bezpečnosť

Legislatívny rámec

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
  - Vykonávací predpis: vyhláška č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe
  - Vykonávací predpis: vyhláška č. 179/2019 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

- Povinné osoby: minimálne bezpečnostné opatrenia sa vzťahujú aj na obce do 6 tisíc obyvateľov.

Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

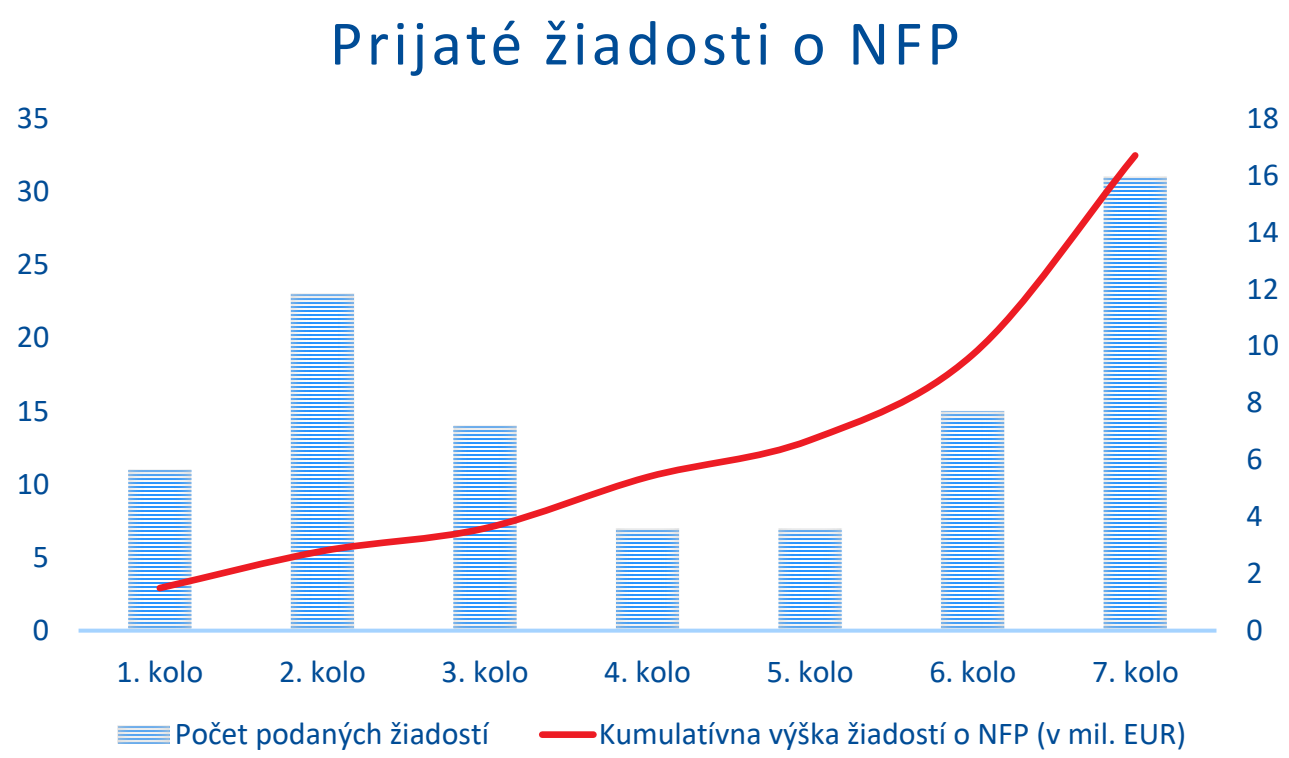
Zdroje financovania

- Operačný program integrovaná infraštruktúra (OPII) 2014-2021
- Plán obnovy a odolnosti (POO) 2021-2026
- Program Slovensko (P SK) 2021-2027

Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

Predbežné vyhodnotenie žiadostí o NFP

Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS (dopytová výzva)



- Prijatých žiadostí spolu: 108
- Z toho územná samospráva: 44
- ½ žiadateľov z územnej samosprávy sa zapojila až v posledných 2 kolách
- K 28.09.2022 bolo u samosprávy zastavené konanie iba v 3 prípadoch

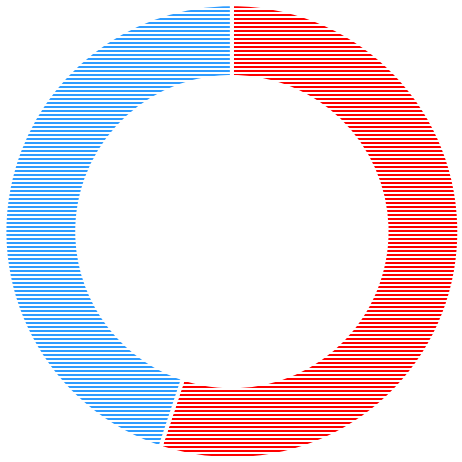
Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

Predbežné vyhodnotenie žiadostí o NFP

Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS

- Výška alokácie po navýšení: 10 000 000 EUR
- Výška predložených žiadostí o NFP: 16 900 213,39 EUR
- Priemerná výška žiadosti o NFP: 197 000 EUR
- Po odstránení duplicitných a žiadostí

Podiel doručených žiadostí o NFP (EUR)



- Územná samospráva
- Ostatné subjekty verejnej správy

Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

Národný projekt „Výcvikové a školiace stredisko pre bezpečnosť prevádzky a správy IT pre sektor VS “

Rozdelený na tri časti:

- Úroveň L1: vzdelávanie pre **zamestnancov VS**
- Úroveň L2: vzdelávanie pre **IT a bezpečnostných pracovníkov vo VS**
- Úroveň L3: **špecializovaný výcvik a školenia** pre IT a bezpečnostných špecialistov v rámci VS

- Realizácia: 2023

Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

POO – Komponent 17, Reforma č. 5: Skvalitnenie vzdelávania a zabezpečenie spôsobilostí v oblasti KIB

Cieľ

Posilniť ľudské kapacity a vzdelávanie v oblasti kybernetickej a informačnej bezpečnosti

- KPI Nárast vyškolených manažérov kybernetickej a informačnej bezpečnosti
- KPI Posilnenie ľudských kapacít a vzdelávania v oblasti kybernetickej a informačnej bezpečnosti

Vytvorenie programu vzdelávania oblasti KIB a zvyšovania bezpečnostného povedomia pre pracovníkov VS v spolupráci s akademickým sektorom

- KPI vytvorenie kompetenčných centier kybernetickej a informačnej bezpečnosti
- KPI Vytvorenie materiálov pre vzdelávanie v oblasti KIB

Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

POO – Komponent 17, Investícia č. 6: Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov

- Základné ciele investície podľa operational agreement:
  - **CID 188:** Zabezpečenie 1000 IT systémov, ktoré budú definované takto: nástroje systému včasného varovania (EWS) budú integrované do systému riadenia incidentov v oblasti kybernetickej bezpečnosti, pričom sa zavedú potrebné hardvérové/softvérové prvky, obojsmerná šifrovaná komunikácia a výstrahy.
  - **CID 189:** Zavádzanie nových alebo revidovaných nástrojov auditu zraniteľnosti verejných IT aplikácií v oblasti kybernetickej bezpečnosti. Posúdenie sa vykonáva prostredníctvom penetračných testov a pomocou softvéru na posúdenie zraniteľnosti, pričom overenie bezpečnostného auditu pre hodnotenie kritickej zraniteľnosti sa musí vykonať vždy pred zavedením. Uprednostnia sa informačné systémy, ktoré sú súčasťou kritickej infraštruktúry.
- Cieľová skupina: orgány verejnej správy
- Ukončenie projektu: 12/2025

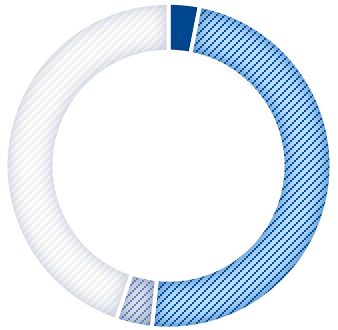
Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

POO – Komponent 17, Investícia č. 6: Posilnenie preventívnych opatrení *Aktivita č. 1 – Vybudovanie Systému včasného varovania (Early warning system)*

- Aktivita bude realizovaná IT projektom v nasledovných oblastiach/častiach:
  - EWS bude zachytávať a zbierať získané informácie z IS VS napojených jednak na Vládny SOC a ďalšie budované centrá inými veľkými rezortmi (účelom je detekcia hrozieb a následné varovanie, ktoré umožní vykonanie opatrení na redukciu rizika)
  - Implementácia nástrojov na zvýšenie kybernetickej bezpečnosti, ktorá bude riešená dvomi časťami:
    - zavedenie log manažmentu na vybraných OVM, ktoré nemajú ambíciu pre vlastné riešenie
    - rozšírenie a dobudovanie bezpečnostného monitoringu prostredníctvom Vládneho SOC-u
  - Rozvoj existujúceho systému na vyhľadávanie zraniteľností Achilles - automatizácia a zrýchľovanie skenovania, tvorby reportov, dátovej analýzy získaných údajov.
- Cieľom je zabezpečiť 1000 IT systémov v prostredí verejnej správy (Vládny SOC + vlastné SOC-y)

ROZPOČET 19,67 mil.

- Systém včasného varovania (SW a osobné náklady)
- Bezpečnosť a monitoring (HW, SW a osobné náklady)
- Systém Achilles (SW a osobné náklady)



Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

POO – Komponent 17, Investícia č. 6: Posilnenie preventívnych opatrení
Aktivita č. 2 – Podpora budovania bezpečnostných dohľadových centier

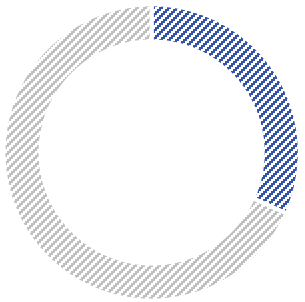
- Na základne výzvy sa budú realizovať samostatné projekty, ktorými budú vybudované, prípadne dobudované dohľadové centrá na veľkých rezortoch (ministerstvá).

- Centrá zabezpečia zber údajov o prevádzke IT systémov v reálnom čase, rozpoznávanie anomálnych aktivít, poskytnutie možnosti skorej detekcie a prípravu protiopatrení na zabezpečenie kybernetickej bezpečnosti a predchádzanie bezpečnostným incidentom => integrácia s EWS.

- Cieľová skupina budú predovšetkým OVM - sektorové rezorty (napr. MH SR, MŠ SR, MZ SR), prípadne Dátové centrum obcí a miest.

ROZPOČET
11 mil.

Výzva "SOC"

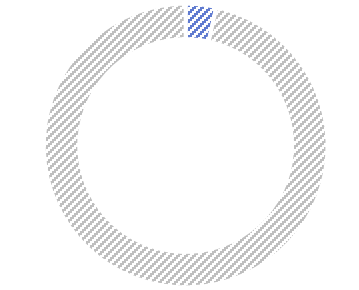


Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

POO – Komponent 17, Investícia č. 6: Posilnenie preventívnych opatrení
Aktivita č. 3 – Overovanie zraniteľnosti ISVS (invazívne, neinvazívne)

- Cieľom aktivity je realizácia intenzívnych a pravidelných overovaní zraniteľnosti a ich vyhodnocovanie (ide o obnovenie služby VJ CSIRT, ktorá na požiadanie túto úlohu vykonávala, ale dnes na to nemá kapacity).
- Kombinácia manuálnych a automatizovaných testovacích nástrojov.
- Externé a/alebo interné typy penetračného testovania na základe žiadosti od subjektov verejnej správy, alebo na základne plánu testovania.
- Overovanie zraniteľnosti bude zamerané na testovanie IS, ktoré sú v prevádzke (prioritne pre základné služby, prvky kritickej infraštruktúry) a nových informačných systémov pred ich spustením.
- Výdavky bude tvoriť refundácia mzdových nákladov na interných zamestnancov, resp. expertov na dohodu.

Rozpočet
1,19 mil.

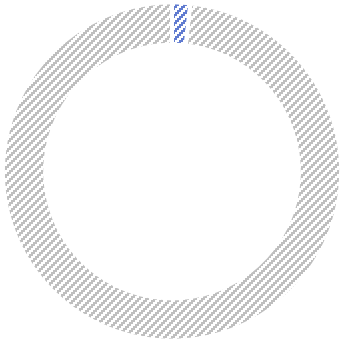


Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

POO – Komponent 17, Investícia č. 6: Posilnenie preventívnych opatrení
Aktivita č. 4 – Realizácia kontroly zákonných povinností správcov ITVS

Rozpočet
0,6 mil.

- Cieľom aktivity je vykonať kontrolu bezpečnosti podľa zákona č. 95/2019 Z. z. o ITVS za účelom overiť skutočnú úroveň stavu kybernetickej a informačnej bezpečnosti vo verejnej správe.
- Kontroly budú vykonávané internými zamestnancami ORKIB priamo u subjektov verejnej správy, ktorí patria napríklad do kategórie II a III podľa vyhlášky č. 179/2020 Z. z.
- Okrem systematickej kontrolnej činnosti budú kontroly vykonávané na podnet alebo z vlastného podnetu (napr. podľa výsledkov zo skenovania zraniteľností...).
- Implementácia jednotného rámca metodických postupov a štandardov pre oblasť kybernetickej a informačnej bezpečnosti vo verejnej správe.

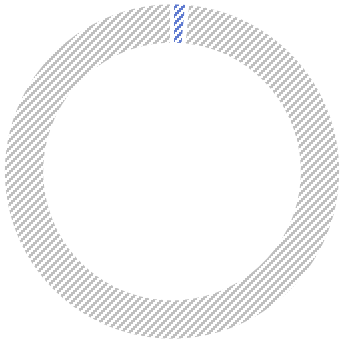


Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

POO – Komponent 17, Investícia č. 6: Posilnenie preventívnych opatrení
Aktivita č. 5 – Program „Bug Bounty“

Rozpočet
0,5 mil.

- Program „Bug Bounty“ predstavuje výzvu pre študentov informatiky alebo príbuzných odborov a odbornú verejnosť na vyhľadávanie a nahlasovanie zraniteľností v informačných systémoch verejnej správy alebo aplikáciách.
- Program bude realizovaný formou súťaže s peňažnými alebo nepeňažnými odmenami.
- Trvanie programu je plánované na tri roky (2023 – 2025).
- Hlavným cieľom je zvýšiť záujem študentov o kybernetickú bezpečnosť, odmeniť talenty a propagovať našu činnosť, poslúži ako časť kampane na zvýšenie publicity o našich aktivitách a povedomí o kybernetickej bezpečnosti.
- Získané informácie o zraniteľnostiach budú odovzdané príslušným orgánom, aby zabezpečili svoje informačné systémy alebo aplikácie.



Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

Ostatné aktivity s realizáciou od roku 2023

- Centrálny portál pre kybernetickú bezpečnosť
  - Základný rozcestník na zorientovanie sa
  - Sústredené všetky informácie na jednom mieste
  - Vzorové smernice a metodické usmernenia
  - Komentovaná legislatíva
- Novelizácia základných právnych predpisov, sprehľadnenie legislatívy
- Dopytová výzva Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS č. 2
- Regionálna podpora manažérov kybernetickej bezpečnosti
- Podpora malých obcí za účelom naplnenia minimálnych bezpečnostných opatrení

Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

Užitočné odkazy

- Vzory bezpečnostnej dokumentácie a metodík, rady pre verejnosť (MIRRI: TU, NBÚ TU)
- Publikácie Vládnej jednotky CSIRT (TU)
- Andraško, Mesarčík, Sokol: Právo kybernetickej bezpečnosti (TU)

- Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (TU)
  - Vzdelávanie: kurzy, workshopy, webináre
  - Certifikácia MKB, Audítor KB
  - Slovník pojmov (TU)

- Vládna jednotka CSIRT (TU)
- Národná jednotka SK-CERT (TU)

Pribinova 25, 811 09 Bratislava
+ 421 2 2092 8559, filip.tubler@mirri.gov.sk

ĎAKUJEME!

www.mirri.gov.sk