Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ČLOVEK AKO RIZIKO AJ RIEŠENIE

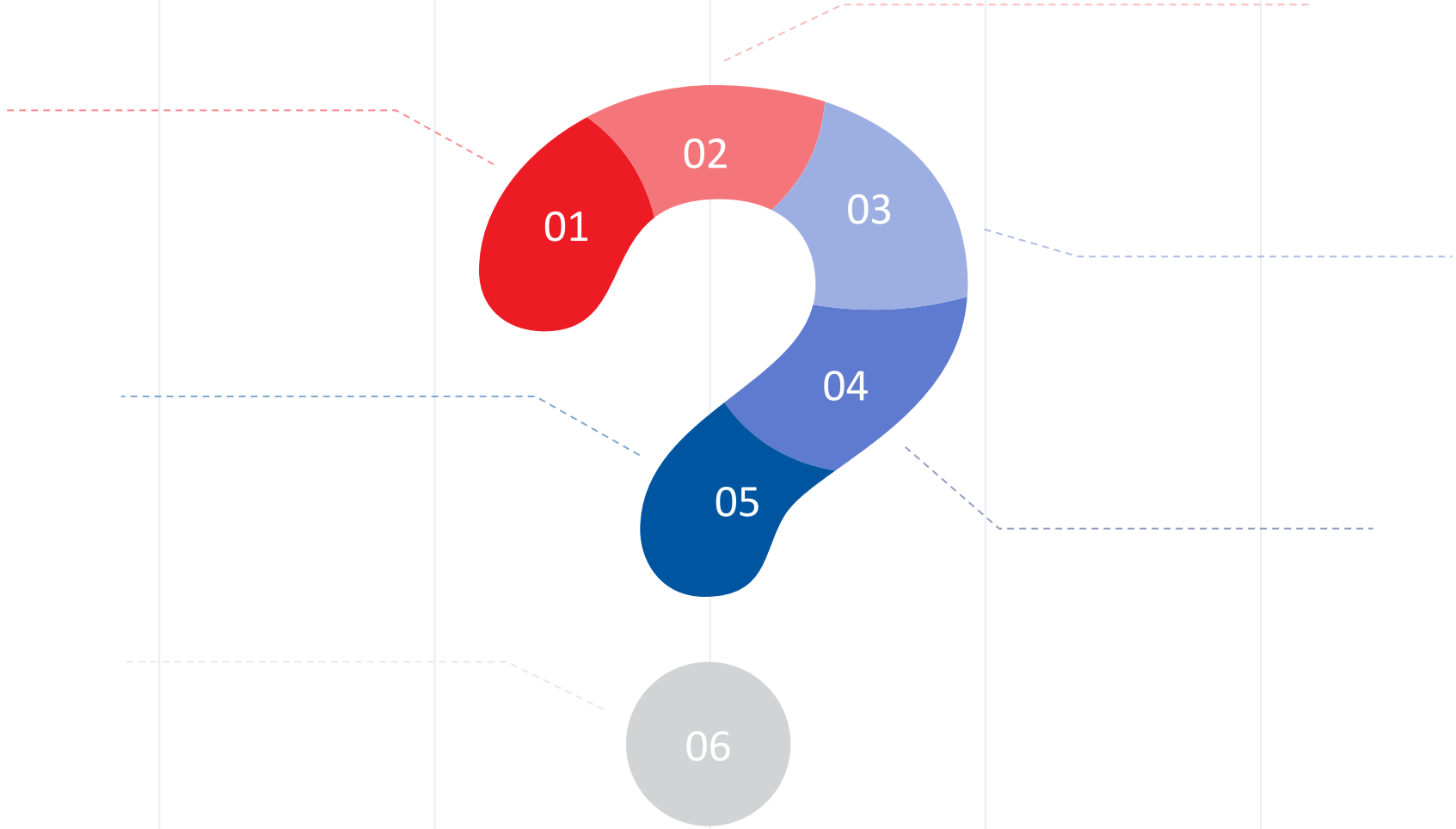
AKO ZVYŠUJEME ODOLNOSŤ KRAJINY VZDELÁVANÍM

26.11.2025
Jesenná Itapa

SEKCIA KYBERNETICKEJ BEZPEČNOSTI
VJ CSIRT ORKIB

Ing. Róbert Bučko
projektový manažér | generálny štátny radca
odbor riadenia kybernetickej a informačnej bezpečnosti | sekcia kybernetickej bezpečnosti

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

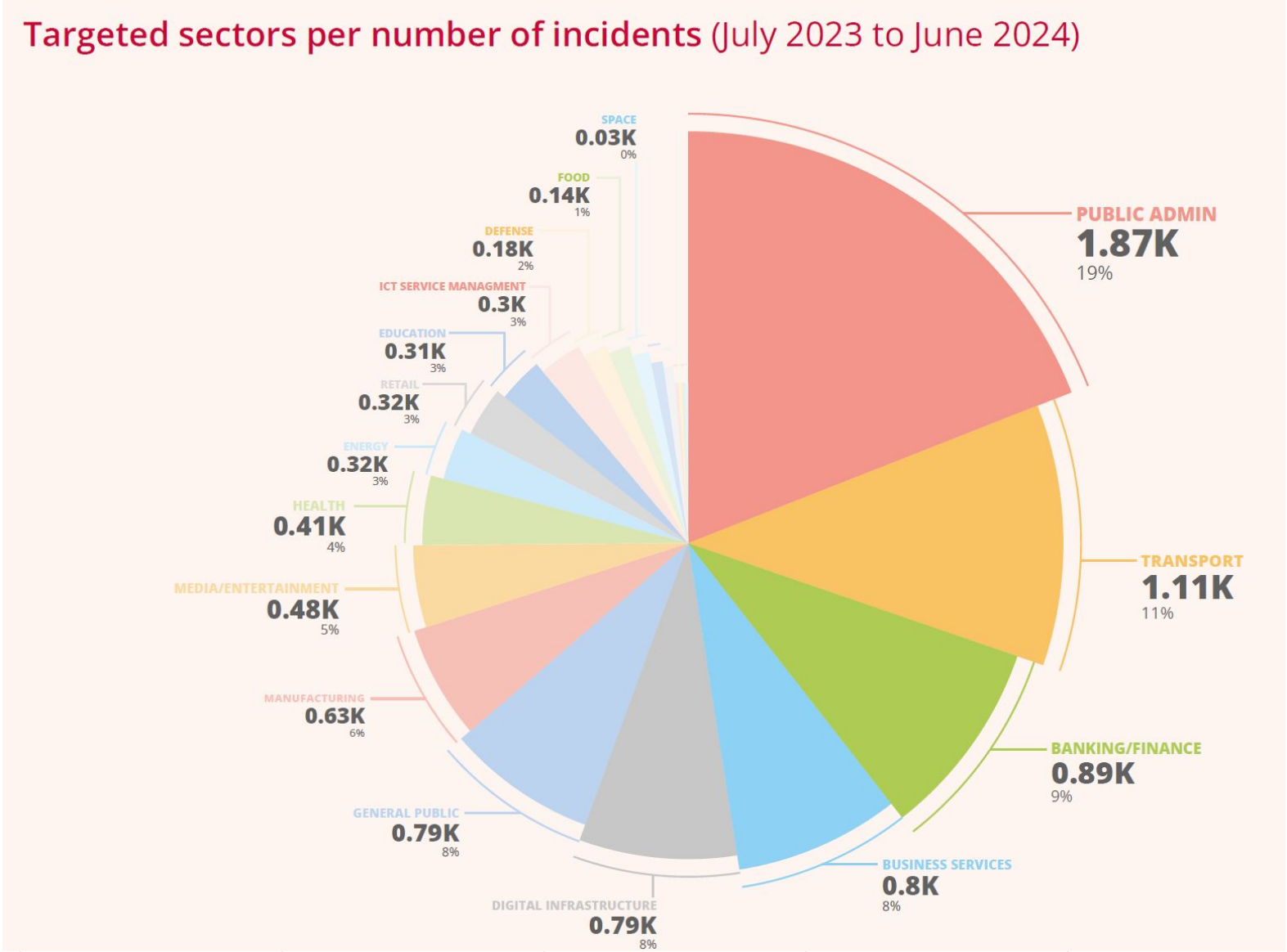


Financované
Európskou úniou
NextGenerationEU

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Najviac kybernetických incidentov:

SUBJEKTY VEREJNEJ SPRÁVY



Zdroj: ENISA - 2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

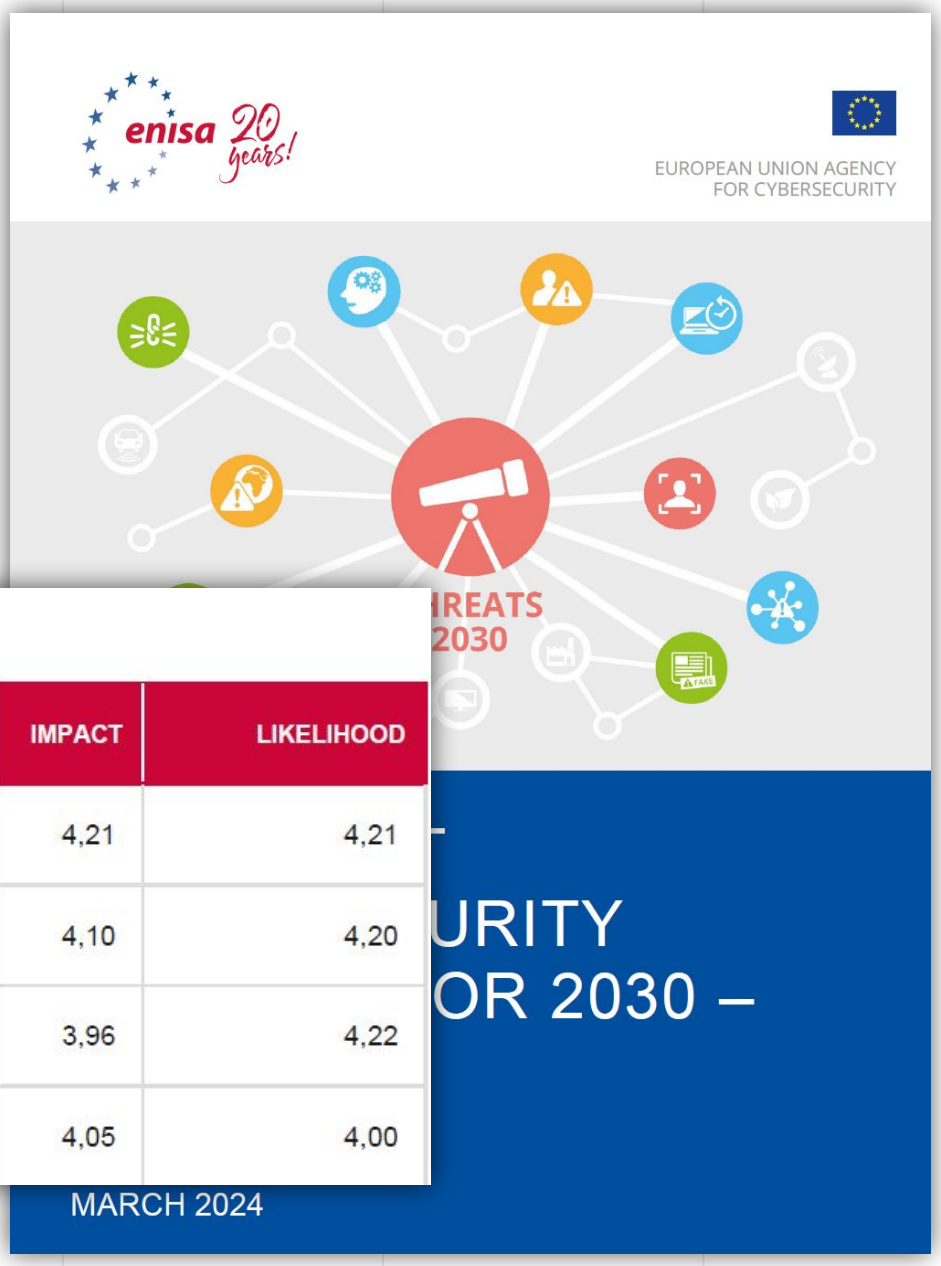
4. THREATS

The real-time Delphi survey, conducted online with the participation of 24 experts, led to the revision of the top ten cybersecurity threats. The experts contributed assessments regarding the impact and likelihood of various threats, providing a comprehensive view of the cybersecurity landscape. The revised top ten list was likelihood scores assigned by the parti

1. Supply Chain Compromise of So
2. Skill Shortage
3. Human Error and Exploited Lega
4. Exploitation of Unpatched and O Ecosystem [New in Top Ten]
5. Rise of Digital Surveillance Auth
6. Cross-border ICT Service Provi
7. Advanced Disinformation / Infl e
8. Rise of Advanced Hybrid Threat
9. Abuse of AI
10. Physical Impact of Natural/Envir

Table 1: New prioritisation of threats

	THREAT	IMPACT * LIKELIHOOD	IMPACT	LIKELIHOOD
1.	Supply Chain Compromise of Software Dependencies	17,71	4,21	4,21
2.	Skill Shortage	17,20	4,10	4,20
3.	Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems	16,69	3,96	4,22
4.	Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [Optional]	16,21	4,05	4,00



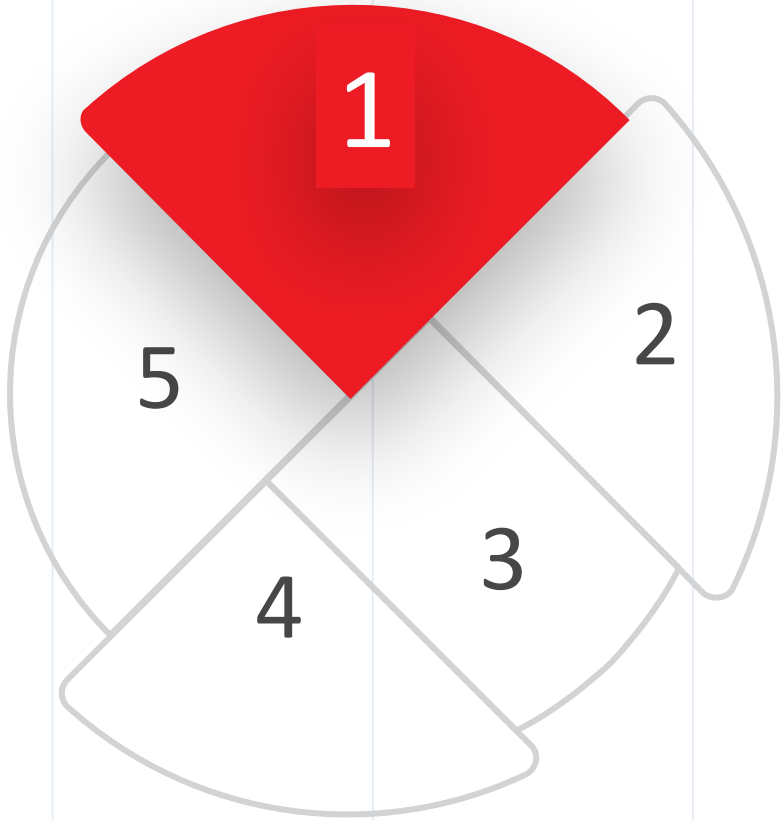
Zdroj: ENISA - FORESIGHT CYBERSECURITY THREATS FOR 2030 – UPDATE

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

RIZIKO MENÍME NA RIEŠENIE

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Sekcia kybernetickej bezpečnosti je funkčne príslušná na plnenie úloh podľa **ZoKB aj ZoITVS.**



Metodická podpora

metodická podpora povinných subjektov,
zvyšovanie spôsobilostí, vzdelávanie,
skvalitnenie a rozvoj KIB v sektore VS

Národný regulátor pre KB v sektore VS

zákonné aj podzákonné normy, vydávanie bezpečnostných štandardov a výkladových stanovísk ITVS, s NBÚ určenie špecifických sektorových identifikačných kritérií, identifikovanie základných služieb a PZS, aktualizácia zoznamu PZS

Strategické vedenie sektora VS

koncepčné a strategické vedenie sektora ITVS,
koordinovanie budovania KIB vo VS

Kritická infraštruktúra

správa podsektora informačné systémy a siete v rámci kritickej infraštruktúry v sektore informačné a komunikačné technológie

Dohľad a kontrola

dodržiavania povinností správcov ITVS,
prijímanie opatrení na nápravu zistených nedostatkov

Financované Európskou úniou
NextGenerationEU

Zdroje financovania

- **OPERAČNÝ PROGRAM INTEGROVANÁ INFRAŠTRUKTÚRA (OPII) 2014-2020 (udržateľnosť projektov)**

- **PLÁN OBNOVY A ODOLNOSTI (POO) 2021-2026**
  - Komponent 17: Digitálne Slovensko
  - Spolu 15 opatrení
  - Rozpočet: 0,55 mld. EUR

- **PROGRAM SLOVENSKO (P SK) 2021-2027**
  - Rozpočet 13 mld. EUR
  - Jednotná metodika, príručka, jedny pravidlá
  - 1 program namiesto 6
  - 1 riadiaci orgán namiesto 6
  - 10 sprostredkovateľských orgánov namiesto 27

EURÓPSKA ÚNIA
Európske štrukturálne a investičné fondy
OP Integrovaná infraštruktúra 2014 – 2020

PLÁN OBNOVY

PROGRAM SLOVENSKO

Pribinova 25, 811 09 Bratislava
robert.bucko@mirri.gov.sk

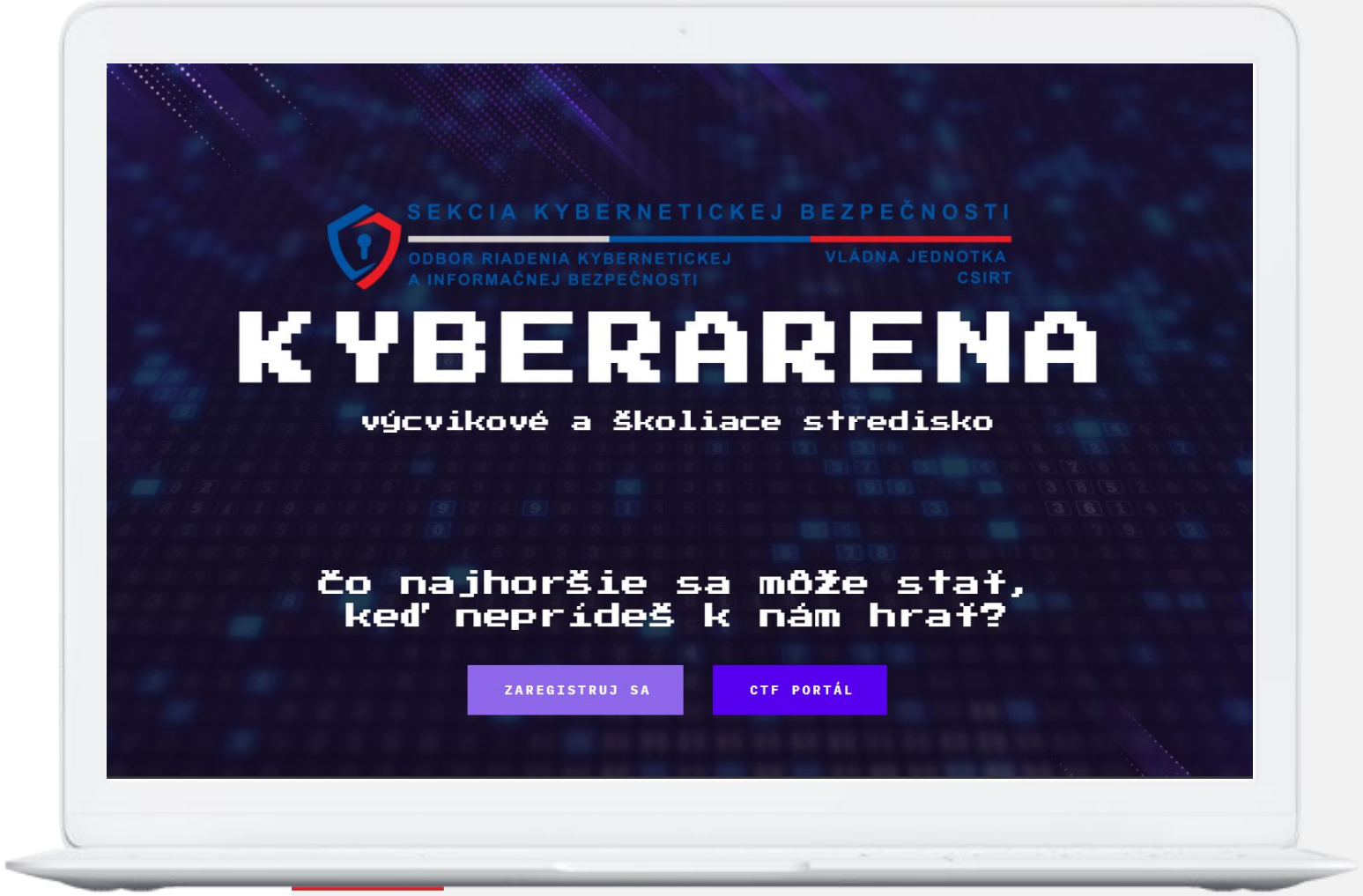
MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Kyberaréna

Primárny cieľ tréningov:
Naučiť sa **logiku za útokmi** a **efektívnu reakciu** na kybernetický incident

KYBERARÉNA MIRRI SR

- **Ako reagovať na kybernetický incident?**
- **Ako identifikovať incidenty?**
- **Ako správne reagovať na rôzne typy incidentov?**

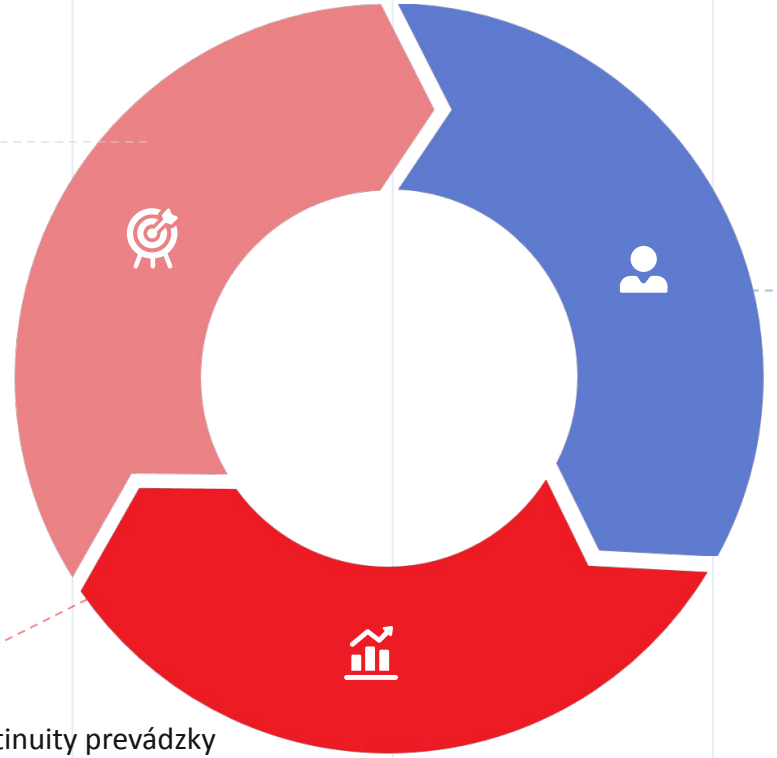


MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Kyberaréna MIRRI SR

CTF Portál

- ❑ Phishingový test
- ❑ Forenzná analýza
- ❑ Reverzné inžinierstvo
- ❑ Cloud
- ❑ Sieťová analýza a iné



Aréna (Red & Blue Team)

- ❑ DDoS
- ❑ Malware, Phishing
- ❑ Kompromitácia
- ❑ Exfiltrácia dát
- ❑ Brute-force
- ❑ Bezpečnostné nástroje

Tabletop Školenia

- ❑ Dezinformácie
- ❑ Phishing
- ❑ Riadenie kontinuity prevádzky
- ❑ Sociálne inžinierstvo

Financované Európskou úniou
NextGenerationEU

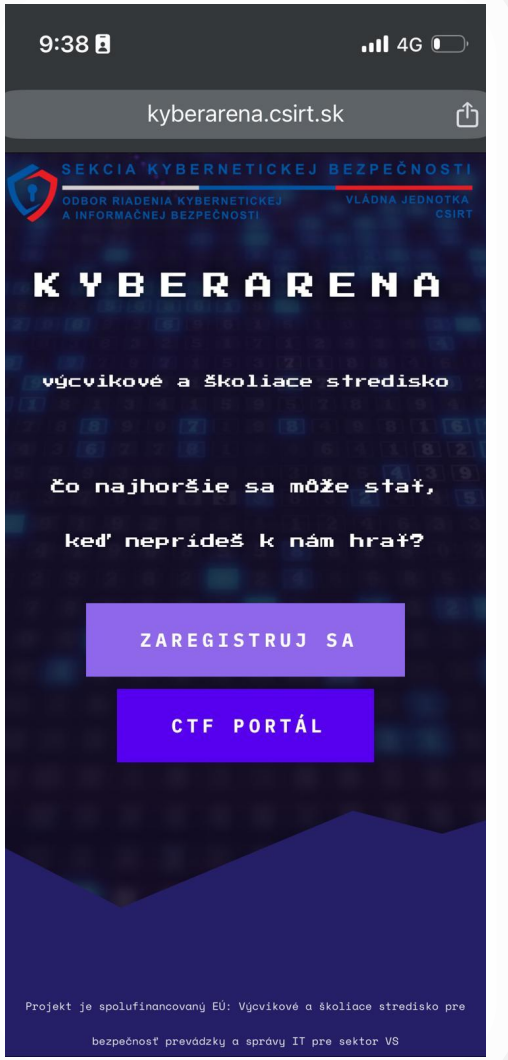
MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Plánujeme preškoliť ďalších:

700+ odborných zamestnancov VS

Udržateľnosť projektu: 5 rokov (2024 - 2028)

Registrácia na tréningy prebieha:
https://kyberarena.csirt.sk



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

POO K17: Reforma Č. 5:

Skvalitnenie vzdelávania a zabezpečenie spôsobilostí v KIB

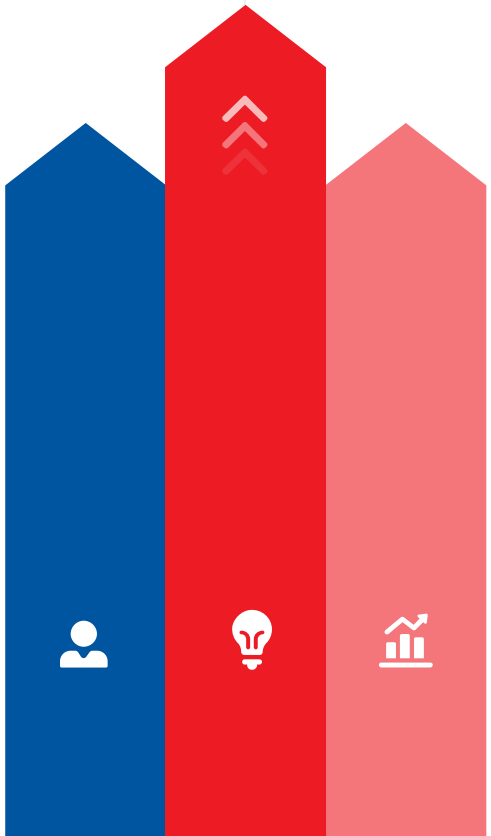
Kompetenčné centrá KB

Vznik **kompetenčných centier** kybernetickej a informačnej bezpečnosti na vysokých školách v SR

Vytvorenie e-learningových materiálov pre vzdelávania v oblasti KIB

Aktivity reformy a základné míľniky:

Posilniť ľudské kapacity
a vzdelávanie v oblasti kybernetickej
a informačnej bezpečnosti



Vyškolenie 600 osôb na úroveň MKB

Nárast vyškolených manažérov kybernetickej a informačnej bezpečnosti – **do 03/2026**

(v zmysle zákona č. 69/2018 Z. z.)

Financované Európskou úniou
NextGenerationEU

POO K17: Reforma č. 5
Kompetenčné centrá kybernetickej bezpečnosti

ŽILINSKÁ UNIVERZITA V ŽILINE

TECHNICKÁ UNIVERZITA V KOŠICIACH

S T U
SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

UNIVERZITA KOMENSKÉHO V BRATISLAVE

UNIVERZITA KONŠTANTÍNA FILOZOFA V NITRE

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
1795 1861
1959

NP Zvýšenie úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti u zamestnancov verejnej správy

Cieľom projektu je vyškoliť odborné kapacity zamestnancov VS na jednotlivé pozície:

1. Tester kybernetickej bezpečnosti
2. Architekt kybernetickej bezpečnosti
3. Špecialista riadenia rizík
4. Špecialista na riadenie kybernetických incidentov
5. Analytik kybernetickej bezpečnosti
6. Audítor kybernetickej bezpečnosti
7. Ostatné pozície

Predpokladaný počet vyškolených zamestnancov VS:

7 430

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Očakávaný prínos vzdelávacích aktivít

11 459

Počet vyškolených zamestnancov VS:
(odborných kapacít KIB)

Pribinova 25, 811 09 Bratislava
robert.bucko@mirri.gov.sk

„Buďte zmenou, ktorú chcete vidieť vo svete.“

- Mahátma Gándhí -

Pribinova 25, 811 09 Bratislava
robert.bucko@mirri.gov.sk

Ďakujem

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SEKCIA KYBERNETICKEJ BEZPEČNOSTI
VJ CSIRT ORKIB

www.mirri.gov.sk

+421 907 107 866
robert.bucko@mirri.gov.sk