MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

SEKCIA KYBERNETICKEJ BEZPEČNOSTI
ODBOR RIADENIA KYBERNETICKEJ
A INFORMAČNEJ BEZPEČNOSTI
VLÁDNA JEDNOTKA
CSIRT

Kybernetická bezpečnosť vo verejnej správe

PROGRAM SLOVENSKO

PLÁN OBNOVY
Financované Európskou úniou
NextGenerationEU

12.5.2025

Postavenie MIRRI SR voči verejnej správe z pohľadu legislatívy

Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe

- Zameraný na dosiahnutie cieľov informatizácie a rozvoja informačných technológií verejnej správy, ktoré vyplývajú z národnej koncepcie a ďalších koncepčných a strategických dokumentov s celoštátnou pôsobnosťou
- MIRRI SR ako orgán vedenia spravuje celú verejnú správu (orgány riadenia) z hľadiska ITVS – približne 8000 subjektov
- Bezpečnosti ITVS sa týkajú paragrafy 18 až 23 zákona

Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti

- Buduje bezpečnostné povedomie, koordinovanú spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore
- MIRRI SR je ústredným orgánom pre sektor 8.3. Verejná správa – do sektora patria všetci správcovia ITVS podľa zákona o ITVS
- Zákon o ITVS je sektorovým bezpečnostným opatrením podľa § 19 ods. 1 zákona o KB

Vízia rozvoja KIB verejnej správy z pohľadu MIRRI SR

Z pohľadu kybernetickej a informačnej bezpečnosti v prepojení na strategické dokumenty (NSKB a NKIVS) vízia MIRRI SR spočíva v oblastiach:

- **Legislatíva**
- **Zvýšenie odolnosti verejnej správy**
- **Štandardizácia dokumentácie**
- **Vzdelávanie zamestnancov verejnej správy**

Legislatíva

1. **Vízia MIRRI SR**
   - Riadiť subjekty verejnej správy prostredníctvom legislatívnych noriem, metodických pokynov a usmernení, za účelom zvyšovania úrovne ich kybernetickej a informačnej bezpečnosti, zohľadňujúc ich výrazne odlišné poskytované služby, organizačné, finančné a personálne zabezpečenie s dôrazom na ochranu kritickej infraštruktúry a kľúčových informačných systémov
   - Poskytovať podporu subjektom ako orgán vedenia, tvoriť národnú koncepciu pre oblasť KB, dohliadať na dodržiavanie zákona v oblasti KB
2. **Prínosy NIS2 voči NIS1**
   - Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii prináša: širší rozsah pokrytých subjektov, nová klasifikácia organizácií, prísnejšie požiadavky na riadenie rizík, prísnejšie požiadavky na hlásenie incidentov, vyššie pokuty za nedodržiavanie predpisov
2. **Transpozícia NIS2**
   - Zákon č. 69/2018 Z.z. bol novelizovaný k 1.1.2025, aktuálne pred MPK novelizácia vyhlášky 362/2018 Z.z. o bezpečnostných opatreniach
3. **Zmeny zákona č. 69/2018 Z.z. v súvislosti s verejnou správou**
   - Vznik nových sektorov 8.1., 8.2., 8.3. Verejná správa
   - Sektorové vyhlášky platia **namiesto** všeobecnej vyhlášky
   - Sektorovou vyhláškou je aj zákon č. 95/2019 Z.z. a jeho vyhláška č. 179/2020 Z.z. pre sektor 8.3. Verejná správa
   - Sektor 8.3. Verejná správa – správcovia a prevádzkovatelia ITVS – **správcami ITVS sú** podľa zákona č. 95/2019 Z.z. **všetky subjekty verejnej správy**
4. **Novelizácia zákona č. 95/2019 Z.z. a vyhlášky č. 179/2020 Z.z.**
   - Vyhláška v procese tvorby, predpoklad zachovania kategorizácie + dôraz na analýzu rizík
5. **Národná koncepcia informatizácie verejnej správy**
   - Aktuálne platná koncepcia z roku 2021, v roku 2025 bude schválená a zverejnená nová koncepcia

Zvýšenie odolnosti verejnej správy

1. **Vízia MIRRI SR**
   - Zvýšiť úroveň bezpečnostných opatrení subjektov verejnej správy tak, aby dokázali v dostatočnej miere a efektívne chrániť svoje informačné systémy a infraštruktúru
   - Vybudovať dostatočne vybavené bezpečnostné dohľadové centrá v ústredných orgánoch verejnej správy, ktoré dokážu efektívne a dlhodobo chrániť zverenú, najmä kritickú infraštruktúru, navzájom spolupracovať a poskytovať služby menším subjektom
2. **Podpora verejnej správy prostredníctvom projektov a výziev zameraných na KIB (Program Slovensko)**
   - Realizované dopytové výzvy:
     - Podpora KIB na regionálnej úrovni pre verejnú správu, vysoké školy a zdravotnícke zariadenia – v realizácii projektov (21 mil. Eur)
   - Národné projekty:
     - Podpora obcí do 6 000 obyvateľov prostredníctvom národného projektu – pripravované (13 mil. Eur)
3. **Podpora odolnosti kritických informačných systémov – ústredné orgány (POO SR a Program Slovensko)**
   - Podpora budovania bezpečnostných dohľadových centier – vybudované 3 nové dohľadové centrá (18 mil. Eur)
   - Zvýšenie úrovne kybernetickej a informačnej bezpečnosti – vo fáze realizácie projektov (20 mil. Eur)
   - Podpora prevádzkovateľov kritickej infraštruktúry – vo fáze realizácie projektov (3 mil. Eur)
4. **Podpora odolnosti MIRRI SR (POO SR a Program Slovensko)**
   - Budovanie systému včasného varovania a rozvoj SOC MIRRI SR/NASES – v realizácii (16 mil. Eur)
   - Zvýšenie úrovne kybernetickej a informačnej bezpečnosti – schválený projekt (3 mil. Eur)
   - Laboratórium excelentnosti kybernetickej bezpečnosti – pripravovaný projekt (4,5 mil. Eur)

PLÁN OBNOVY

Financované Európskou úniou NextGenerationEU

PROGRAM SLOVENSKO

Štandardizácia dokumentácie

1. **Vízia MIRRI SR**
   - Zabezpečiť štandardizované, bezplatné a aktuálne dokumenty pre verejnú správu za účelom zvýšenia počtu subjektov s dostatočne kvalitnou dokumentáciu, ktorej zavedením dôjde k zvýšeniu úrovne kybernetickej a informačnej bezpečnosti subjektov a súladu so zákonom
   - Sekundárnym efektom je jednoduchšia implementácia, zníženie nákladov, odstránenie potreby využívania služieb tretích strán
2. **Centrálny portál kybernetickej bezpečnosti**
   - Štandardizované dokumenty k dispozícii subjektom verejnej správy
   - Dôležité upozornenia a novinky v oblasti KIB
   - Kategorizácia subjektov
   - Vzdelávanie a osveta (vzdelávacie články, návody)
3. **Štandardizácia dokumentov – Jednotný metodický rámec**
   - Viac ako 100 aktuálnych dokumentov pre subjekty verejnej správy - smernice, metodiky, vzory
   - Aktualizácia dokumentov pri novelizácii relevantných noriem
   - Personalizované formuláre a dokumenty
   - Všetky dokumenty sú k dispozícii bezplatne verejnej správe
   - Nové dokumenty pribudnú v máji 2025 a Q3/2025

https://kyberportal.slovensko.sk

PLÁN OBNOVY

Financované Európskou úniou NextGenerationEU

Tieto úlohy sú realizované projektom Štandardizácia technických a procesných riešení KIB (POO SR, K17, R4)

Vzdelávanie zamestnancov verejnej správy

1. **Vízia MIRRI SR**
   - Uvedomujúc si výrazný nedostatok odborníkov KIB vo verejnej správe a nedostatočné povedomie o problematike KIB MIRRI SR podporuje prostredníctvom legislatívy, projektov, vzdelávania a osvety rozvoj personálnych kapacít v rôznych cieľových skupinách (študenti základných až vysokých škôl, bežní zamestnanci vo verejnej správe, odborní zamestnanci, verejnosť)
2. **Reforma Skvalitnenie vzdelávania a zabezpečenie spôsobilostí v oblasti KIB (POO SR, K17, R5)**
   - Vzdelávanie manažérov kybernetickej bezpečnosti – v procese verejného obstarávania
   - Vznik vzdelávacích materiálov pre e-learning bežných zamestnancov verejnej správy – realizácia verejného obstarávania - vyhodnotenie
   - Kompetenčné centrá kybernetickej bezpečnosti – projekty šiestich vysokých škôl:
     - Vytvoria študijné programy v oblasti KIB
     - Spúšťajú bezplatné vzdelávanie pre zamestnancov verejnej správy
     - Spolupracujú pri výskume, vývoji a pri tvorbe projektov v KIB
     - Podporujú stredné školy v zavádzaní výučby v oblasti KIB
3. **Kybernetická aréna MIRRI SR**
   - Špecializovaný výcvik (Red team vs. Blue team) najmä pre odborníkov bojujúcich proti útokom
   - Otvorená pre celú verejnú správu, prihlasovanie dostupné cez **https://kyberarena.csirt.sk/**
   - Tabletop školenia najmä pre manažérov
   - Capture the flag portál – phishing, cloud, forenzná analýza, reverzné inžinierstvo
   - Financované z projektu OPII Výcvikové a školiace stredisko pre bezpečnosť prevádzky a správy IT pre sektor VS

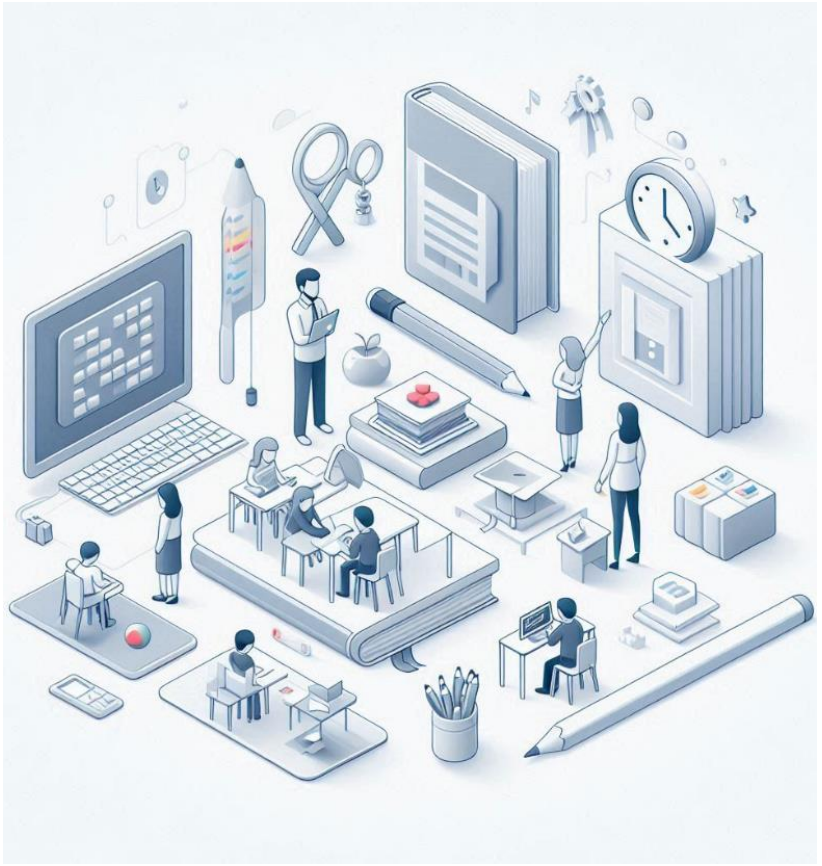
https://kyberarena.csirt.sk

PLÁN OBNOVY

Financované Európskou úniou NextGenerationEU

Vzdelávanie zamestnancov verejnej správy

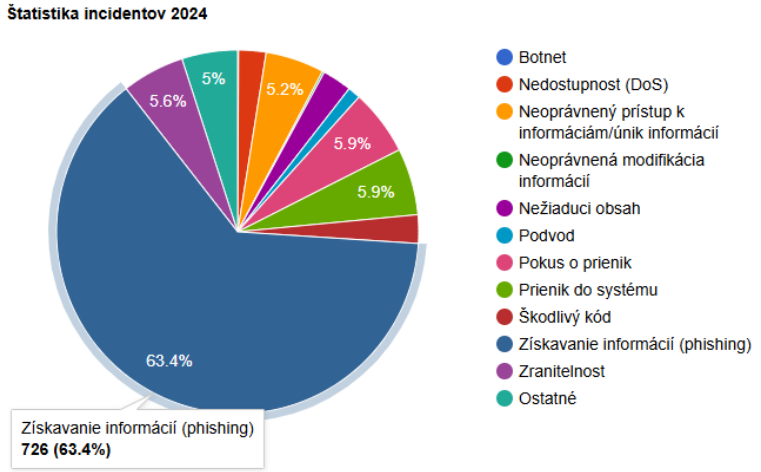
4. **Národný projekt „Zvýšenie úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti u zamestnancov verejnej správy“**
   - Vzdelávanie bežných zamestnancov, ako aj odborníkov v KIB od všeobecných školení po špecializované až na úroveň audítorov kybernetickej bezpečnosti
   - Typy školení: governance, technické a špecializované školenia
   - Pre celú verejnú správu a bezplatne
   - Celkovo viac ako 7400 osoboškolení
   - Projekt je schválený a začiatok realizácie je predpokladaný v Q3/2025
5. **Ďalšie aktivity MIRRI SR**
   - Školenia na stredných školách a ďalších subjektoch – základy bezpečnosti, kyberšikana, phishing
   - Špecializované konferencie pre verejnú správu – Kybertour 2025 (8 krajských miest počas roka 2025)
   - Komunikácia so subjektami prostredníctvom Centrálneho portálu kybernetickej bezpečnosti – články, dokumenty, odkazy na vzdelávanie
   - Obsah určený aj pre širokú verejnosť – pripravované rozhovory s odborníkmi – videá na internete, hybridné hrozby
   - Vzdelávanie odborníkov MIRRI – školenia, medzinárodná spolupráca



Odporúčania pre OVM vzhľadom na súčasnú situáciu v KB

1. **Riešte bezpečnosť proaktívne** (nie reaktívne)
2. **K odstraňovaniu zraniteľností** pristupujte **zodpovedne**
   - **Bezodkladné odstraňovanie zraniteľností**, najmä kritických a aktívne zneužívaných
   - Udržiavať **aktuálny zoznam aktív organizácie** (aby ste vedeli, čo máte chrániť) v systéme **Vládny informačný systém kybernetickej bezpečnosti (VISKB)**
3. **Obmedzte pripájania na interné systémy výhradne prostredníctvom zabezpečeného a šifrovaného pripojenia**
   - Používate **silné a rozmanité heslá**, zariadenia udržiavajte (alebo ich vyraďte), aj keď sa už nepoužívajú tak často
   - Používateľom a administrátorom pridávajte **len nevyhnutné oprávnenia** na prácu (pomôže v prípade kompromitácie)
   - Použite virtuálne privátne siete (VPN), použite **viacfaktorovú autentifikáciu,** a dbajte na **odporúčania VJ CSIRT**
4. **Systémy pravidelne aktualizujte a vykonávajte aj hardening** alebo **penetračné testovanie**
   - Nahlásené opravy a odporúčanie vždy implementujte a v prípade nejasností, nápravu konzultujte
5. **Aktualizujte aj zamestnancov, nielen systémy**
   - Poskytujte (alebo sa prihláste na) pravidelné školenia na zvýšenie povedomia o kybernetickej bezpečnosti
   - Školenia nech sa realizujú pravidelne, praktickou formou, aby to malo pre zamestnancov prínos (pozor na **phishing**)
6. **Zapojte sa do bezpečnostného monitoring a aktivne sa podieľajte na jeho ladení**
   - Zariadenia, ktoré sú zapojené do bezpečnotného monitoringu sú lepšie chránené voči aktivitám aktérov hrozieb (napr. pokusom o prienik)
   - Pravidelný reporting bezpečnostných udalostí, ktoré boli zachytené v rámci monitoring (ak využívate SOC ako službu, pýtajte si ho od dodávateľa a sledujte zmeny)

CSIRT.SK



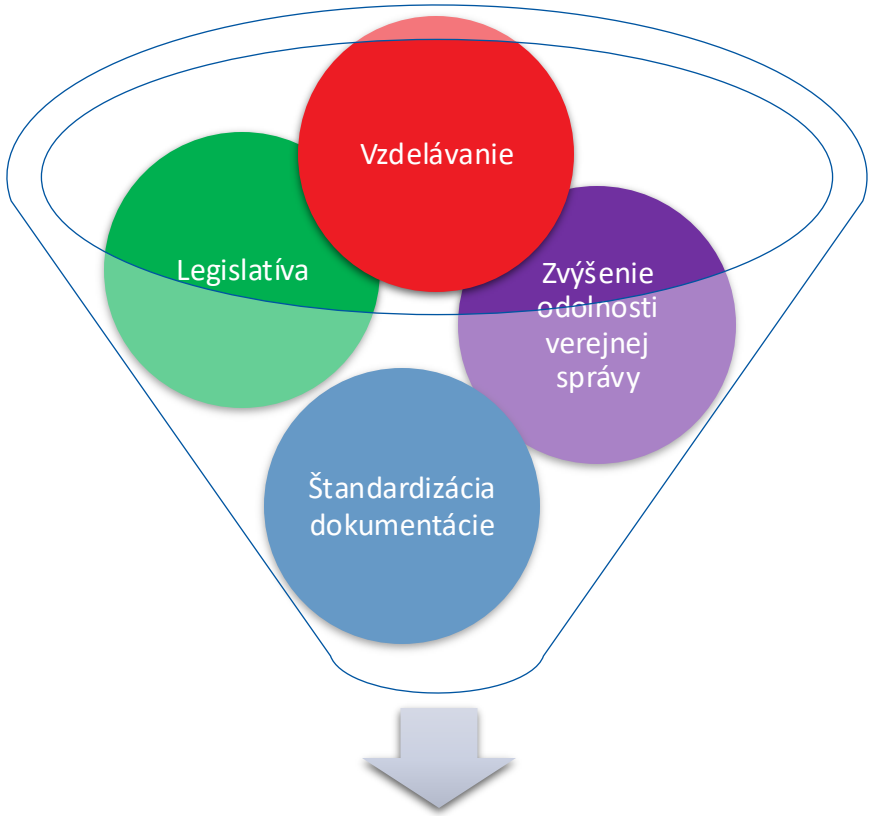
Odporúčame takisto využívať ponúkané služby SKB MIRRI

1. **Riešenie bezpečnostných incidentov a konzultácie v prípade zabezpečenia organizácie**
   - V prípade kybernetického bezpečnostného incidentu sú vytvorené odporúčania, ktoré ste prehliadli a je potrebné ich bezodkladne implementovať
   - Chcete zlepšiť svoju bezpečnosť, máte na to nástroje, ale neviete či to robíte správne?
   - Nastavili ste si zabezpečenie, ale neviete či ste dostatočne chránení?
2. **Kyberaréna**
   - **Pre zvyšovanie povedomia o kybernetickej bezpečnosti sa prihláste do Výcvikového a školiaceho strediska (VaŠS)**
   - Môžete sa vzdelávať v procesných témach, pre manažérov a vedúcich
   - Môžete sa vzdelávať technicky, bude odolávať pokusom o prienik útočníka do Vašej organizácie
3. **Achilles**
   - Na začiatok sa stačí zaregistrovať a pridať svoje aktíva (dostupné zo siete Govnet / Internet) do **VISKB**
   - Získate **pravidelné hlásenie o zraniteľnostiach** vo Vašej organizácii
   - Vašou úlohou je nahlásené nedostatky zapracovať v čo najkratšom možnom čase
   - Pokiaľ máte záujem o hĺbkové testovanie systému, môžete využiť službu **Ares** (službu penetračného testovania)
4. **Využívajte službu overenie úniku prihlasovacích údajov (napr. Have I Been Pwnd)**
   - Neviete, či v rámci nedávneho úniku prihlasovacích údajov neunikol aj Vás mail?
   - Na overenie úniku prihlasovacích údajov pre konkrétnu doménu využite službu Have I Been Pwnd
5. **Bezpečnostný monitoring a monitoring hrozieb:**
   - Zvyšujete odolnosť voči kybernetickým útokom prostredníctvom systému včasného Varovania
   - Monitoring kanálov útočníkov (napr. na sieti Telegram), aby bolo možné sa na DDoS kampane pripraviť a odolať im
6. **Odporúčania, návody, varovania, prehľady a metodiky sú zverejňované na webovom sídle Kyberportálu a VJ CSIRT**

Kybernetická bezpečnosť vo verejnej správe

https://kyberportal.slovensko.sk

https://csirt.sk



Výrazné zvýšenie úrovne kybernetickej bezpečnosti verejnej správy

https://kyberarena.csirt.sk

PLÁN OBNOVY

Financované Európskou úniou NextGenerationEU

PROGRAM SLOVENSKO

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

www.mirri.gov.sk

PhDr. JUDr. Mgr. Ervín Šimko, MSc., MBA, LL.M