MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

ITAPA | 10. 11. 2021

Trendy kybernetickej a informačnej bezpečnosti vo verejnom sektore

Martin Florián, PhD.
generálny riaditeľ sekcie kybernetickej bezpečnosti

Obsah

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Súčasný stav v kybernetickej a informačnej bezpečnosti (KIB) vo verejnej správe (VS)

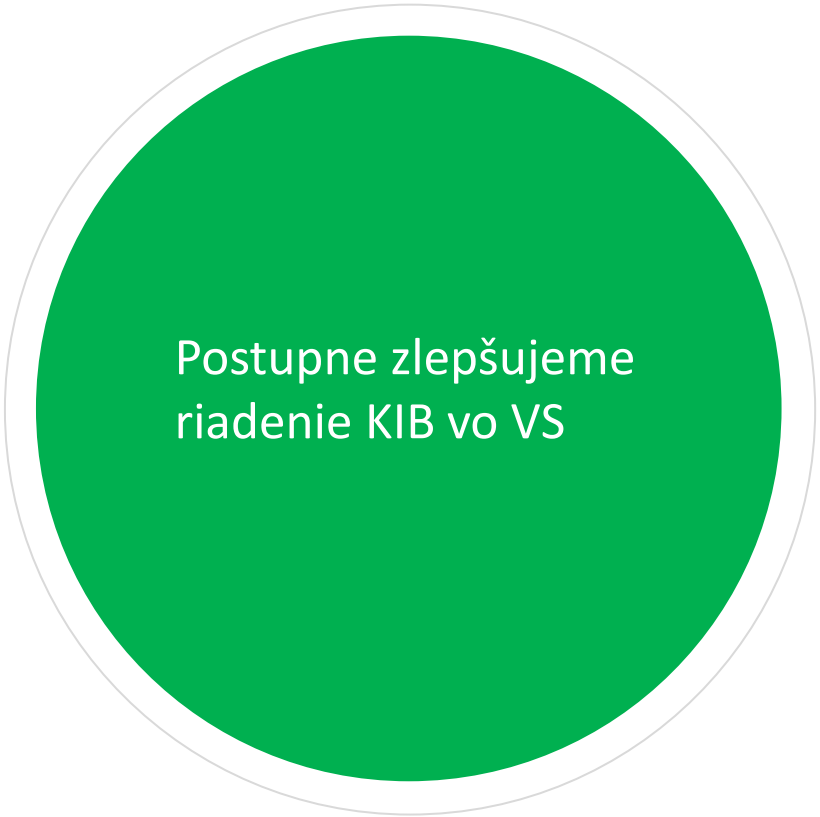
Hlavná výzva KIB vo VS je **slabé povedomie** a **málo spôsobilých ľudí (Brainware)**

Súčasný stav nie je optimálny; to ale neznamená, že nie je na čom stavať.

- Verejná správa a jej informačné systémy sú najviac zraniteľné cez **ľudský faktor** (phishing, sociálne inžinierstvo, prístupové práva, slabé heslá, ...).
- Inštitúciám chýbajú potrebné **kvalifikované ľudské zdroje** pre oblasť IB a KB.
- V drvivej väčšine OVM (orgánov verejnej moci) bol síce menovaný **MKB (manažér kybernetickej bezpečnosti)**, ale väčšinou išlo len o preradenie človeka z inej pozície bez **„security background-u“** a bez podpory ďalším personálom. Podobná situácia je aj v iných expertných roliach KIB.
- KIB školenia a tréningy sú zatiaľ **málo koncepčne plánované**.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Zmeny a zlepšenia kybernetickej a informačnej bezpečnosti (KIB) vo verejnej správe (VS)

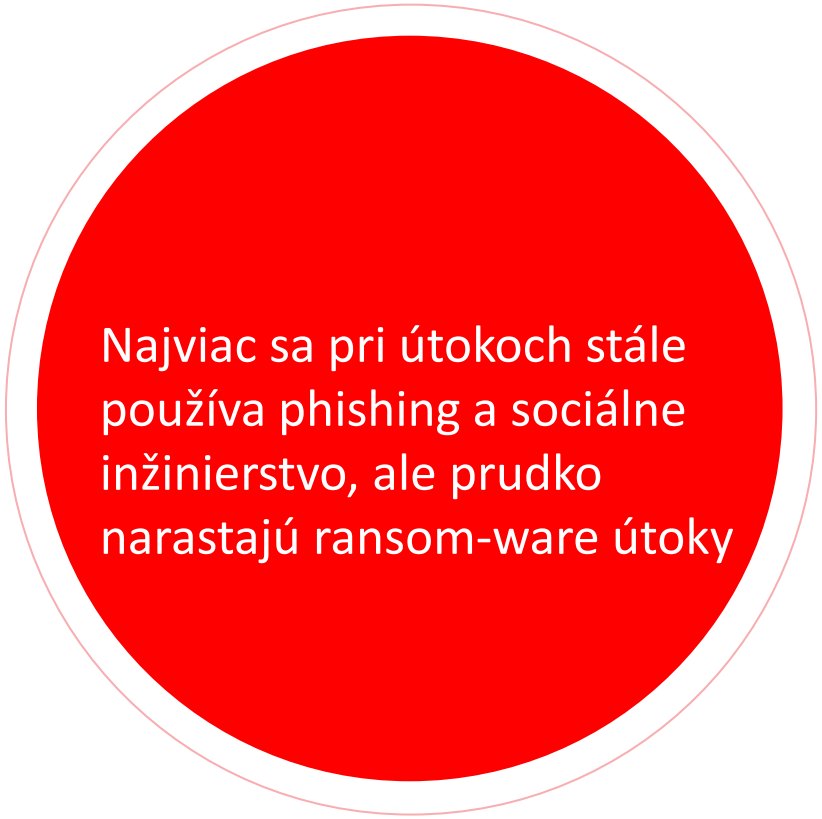


Pozitívne zmeny pre KIB vo VS :

- **Technické a personálne posilnenie** SKB v kľúčových spôsobilostiach
- **Design spoločného SOC (Security Operation Center) pre VJ CSIRT a NASES**
- **Horizontálna dopytová výzva pre zlepšenie governance** a úrovne KIB v ISVS
- Zvyšovanie úrovne bezpečnosti v kybernetickom priestore VS prostredníctvom **dobudovávania spôsobilosti vládnej jednotky CSIRT.SK** v súvislosti s **defenzívnou aj ofenzívnou analytickou činnosťou** ako aj asistencie pri **riešení** kybernetických bezpečnostných incidentov vo verejnej správe.
- Zlepšovanie detekcie zraniteľností aj ich systematického odstraňovania a zmierňovania pomocou platformy **Achilles**.
- Národné **projekty** aj **dopytové výzvy** majú postupne posilnené KIB dimenzie
- Vytvorenie **KIB „templatov“ a šablón** pre OVM v zmysle vyhlášky 179/2020
- **Príprava KIB reforiem v POO** (Plán obnovy a odolnosti)
- Participovali sme na príprave Národnej stratégiu kybernetickej bezpečnosti (schválená vládou SR 7. januára 2021) a na príprave Akčného plánu NSKB

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Trendy kybernetických útokov a riadenia KIB



V kontexte pandémie COVID-19, rastúcemu režimu Home Office sa menia patterny kybernetických útokov a hrozieb.

- Informačné systémy sú stále najviac ohrozované cez **Phishing a Sociálne inžinierstvo** (cca 44% útokov na ISVS za posledný rok)
- Posledné 2 roky prudko narástli **Ransom-ware** incidenty a hrozby
- **Cloud Security** narastá na dôležitosti
- Rýchly nástup **Umelej inteligencie (AI)**
- Keďže podľa kvalifikovaných odhadov (Štúdia (ISC) 2 Cybersecurity Workforce) zchýba na globálnom trhu asi 4 milióny KIB profesionálov, je potrebné **automatizovať cez RPA (Robotic Process Automation)** všetky činnosti, ktoré je možné a zmysluplné automatizovať

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Plánované kroky a iniciatívy pre lepšie riadenie kybernetickej a informačnej bezpečnosti (KIB) v POO (Pláne obnovy a odolnosti)

KIB reformy a investície v Pláne obnovy a odolnosti:

- **Štandardizácia** technických a procesných riešení (štandardizácia dizajnu, vývoja a zabezpečenia, aby bolo možné testovanie a certifikácia podľa objektívnych kritérií)
- Skvalitnenie **vzdelávania** a zabezpečenie spôsobilostí v oblasti kybernetickej a informačnej bezpečnosti (Brainware, Risk Mitigation Attitude, Security Capabilities)
- Posilnenie **preventívnych** opatrení, **zvýšenie rýchlosti detekcie** a **riešenia** incidentov (včasná detekcia prvých patternov, early warning systémy, zlepšenie časov odozvy aj nápravy)
- Rekonštrukcia a **dobudovanie zabezpečených priestorov** s kritickou infraštruktúrou (pre KIB systémy, procesy a dokumentáciu v špeciálnom režime)

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Koncepcia riadenia kybernetickej a informačnej bezpečnosti (KIB) vo verejnej správe (VS)

Stratégia riadenia KIB vo VS má byť konzistentná s Národnou stratégiou KB (NSKB)

SKB je zodpovedná za implementáciu NSKB pre ISVS:

Hlavné **princípy** navrhnutých KIB cieľov :

- **Posilnenie pripravenosti** VS na kybernetické hrozby
- Efektívne **odhaľovanie** (detekcia) aj **objasňovanie** hrozieb a zraniteľností KIB
- Zvýšenie **odolnosti** (resilience) IS verejného sektora
- Bezpečné a **zabezpečené služby** poskytované ISVS (dostupné a dôveryhodné)

Koncepcia riadenia KIB sa venuje primárne týmto oblastiam:

- **Prepojenie bezpečnostnej architektúry a riadenia** KIB **požiadaviek**.
- KIB projekty sa musia **metodicky riadiť na úrovni projektového a programového portfólia.**
- Definovanie **jasných politík a metodík** pre obstarávanie aj pre KIB oblasti.
- Posilnenie požiadaviek KIB pre riadenie **strategických cross-rezortných iniciatív**.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Koncepčné ciele kybernetickej a informačnej bezpečnosti (KIB) vo verejnej správe (VS)

Koncepčné ciele pre KIB vo VS :

- Posilnenie **preventívnych** riešení a lepšia **analýza** KIB relevantných **dát**
- **Prilákanie a udržanie kvalitných ľudí s KIB profilom** do VS - **vytvorením podmienok pre ich motiváciu a profesionálny rast** v oblasti kybernetickej a informačnej bezpečnosti - so zámerom väčšej konkurencie-schopnosti voči súkromnému sektoru - **pomocou kombinácie vhodných faktorov** ako je primerané ohodnotenie, zabezpečenie **kvalitných školení** aj možnosti riešenia **zaujímavých** úloh vyžadujúcich **kreatívne** myslenie.
- Zvyšovanie úrovne bezpečnosti v kybernetickom priestore VS prostredníctvom dobudovávania spôsobilosti vládnej jednotky CSIRT.SK v súvislosti s **defenzívnou aj ofenzívnou analytickou činnosťou** ako aj asistencie pri **riešení** kybernetických bezpečnostných incidentov vo verejnej správe.
- Národné **projekty** aj **dopytové výzvy** musia mať posilnené KIB dimenzie vo všetkých fázach implementácie a nasadenia (**Security by Design**).
- Modelovanie, udržiavanie a rozvoj **bezpečnostnej architektúry**. Najmä **budovanie centrálnych – spoločných blokov bezpečnostnej architektúry**, ktoré budú môcť byť využité jednotlivými OVM.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Princípy pre riadenie kybernetickej bezpečnosti vo verejnej správe

1. Posilnenie internej profesionality a zodpovednosti

- **Kľúčové spôsobilosti**, zručnosti a skúsenosti majú byť hlavne u **interných** zamestnancov.
- **Vlastníctvo kvality (ownership) a zodpovednosti (empowerment)** má byť posilnené na všetkých úrovniach riadenia.
- Budovanie kľúčových kapacít a schopností pre zabezpečenie KIB na organizačnej, metodickej, procesnej aj analytickej úrovni.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Princípy pre riadenie kybernetickej bezpečnosti vo verejnej správe

2. Demonopolizácia a redukcia vendor lock-in väzieb

- Je potrebné **skončiť monopoly, rajonizáciu** oblastí a programov medzi dodávateľmi
- **Zdrojové kódy SW, architektúra** riešenia a kvalitná dokumentácia dodaných riešení má byť **vo vlastníctve štátu**.
- **Súťaž a rovnosť šancí** má tlačiť potenciálnych dodávateľov k vyššej kvalite a k primeranej cene.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Princípy pre riadenie kybernetickej bezpečnosti vo verejnej správe

3. Zabezpečenie kvality a maximalizácia CBR

- Cieľom je **maximalizovať** pomer **hodnota/cena**.
- Zlepšiť **kvalitatívne** aj **kvantitatívne** KIB **kritériá** pre vyčíslenie celkových **benefitov** aj celkových **nákladov** na projekty a riešenia.
- Pri technologických riešeniach treba viac myslieť na **investície do ľudských spôsobilostí** potrebných pre maximálne **zužitkovanie potenciálu** implementovaných riešení a systémov.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Princípy pre riadenie kybernetickej bezpečnosti vo verejnej správe

4. Viac modularity a fázovania vo veľkých projektoch

- Veľké projekty by sa mali **segmentovať** a fázovať na menšie moduly, kde pokračovanie v ďalšej fáze projektu by malo byť podmienené kvalitnou a úplnou dodávkou predchádzajúcej fázy.
- Mal by sa viac zaviesť **PoC** (Proof of Concept) model na báze **MVP** (Minimal Viable Product).
- Minimalizácia riskantných Big Bangov.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Priority kybernetickej a informačnej bezpečnosti vo verejnej správe

1. Zmena kultúry a integrity na všetkých úrovniach KIB

- Stredné aj nižšie riadiace kádre potrebujú vidieť a zažiť autentický „**Leadership**“ a dobrý **osobný príklad** vo vedení.
- Boj s hrozbami a s útočníkmi je o **integrite, motivácii a dôveryhodnosti konkrétnych ľudí** viac ako o dokonalosti KIB procesov.
- Je dôležité **monitorovať trendy** a zapájať viac **meranie** a objektívnu **kvantifikáciu**.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Priority kybernetickej a informačnej bezpečnosti vo verejnej správe

2. Väčšia jednoduchosť a zrozumiteľnosť

- Čím komplikovanejšie procesy riadenia KIB, tým väčší priestor pre nepochopenie nejednoznačné interpretácie.
- Legislatíva a metodické usmernenia pre KIB musia byť **jednoznačné**, **konzistentné**, **harmonizované** a **zrozumiteľné**.
- Naplnenie týchto kritérií pri dodávkach, metodikách a projektoch.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Priority kybernetickej a informačnej bezpečnosti vo verejnej správe

3. Osveta a jasná komunikácia KIB princípov a cieľov

- Témy KIB a zmierňovanie KIB rizík **nesmú byť témou len pre zopár top expertov**.
- Je potrebné na všetkých úrovniach organizácie systematicky **komunikovať princípy, ciele a zmysel** týchto KIB iniciatív.
- Komunikácia má byť nastavená a **primeraná na cieľový segment**.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

Priority kybernetickej a informačnej bezpečnosti vo verejnej správe

4. Väčšia proaktivita v riadení KIB a zapájanie predikcie

- **Proaktivita** musí postupne rásť na úkor drahšej reaktivity.
- Treba posilniť **včasnú detekciu prvých signálov** hrozieb a zraniteľností.
- **Umelá inteligencia** by mala nahrádzať a odľahčiť ľudské kapacity všade tam, kde je to možné.
- **Dátová integrácia** a **dátová analytika** by mala zefektívniť fázy detekcie aj riešenia incidentov, ako aj posilniť proaktívne opatrenia.

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

DISKUSIA

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

ĎAKUJEME!


MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Back-up slides

Priority KIB vo VS

- **Zjednotenie formálnych požiadaviek** na riešenie jednotlivých oblastí kybernetickej bezpečnosti
- **Riadenie rizík** pre ISVS
- **Inteligentné systémy a technické riešenia** - založené na centrálne spravovanej metodike pre kvalitatívnu analýzu rizík a katalógu hrozieb
- **Centralizované riadenie kontinuity činností**, vrátane realizácie vyhodnotenia dopadov pre jednotlivé komponenty, ako aj plánovanie náhradného výkonu (napríklad nedostupnosť platformy dátovej integrácie), koordinácia havarijného plánovania a pod.
- Návrh programov zvyšovania **bezpečnostného povedomia a zručností používateľov** (interných aj externých)
- Centrálne **riadenie požiadaviek** na bezpečnosť u dodávateľov IT riešení pre verejnú správu
- Zavedenie režimu nepretržitého výkonu **auditu** bezpečnosti prevádzkovaných riešení
- Podpora **inovácií štandardov** a riešení v oblasti identifikácie, autentifikácie, autorizácie a vytvárania záznamov
- Návrh špecifických systematických riešení ochrany údajov pri realizácii princípu "**jedenkrát a dosť**", najmä v oblasti ochrany osobných údajov a riadenia prístupu k údajom

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk

KIB Vízia vo VS

Rýchle riešenie kritických problémov KIB v štáte a v ISVS

(v rámci platnej legislatívy, prostredníctvom vzdelávania, štandardizácie, koordinácie činnosti, podporou existujúcich pracovísk)

Stanovenie priorít pre systematické riešenie KIB ISVS

(závisí od dostupných zdrojov a malo by sa prehodnocovať raz ročne)

Priebežná objektivizácia a upresňovanie údajov o stave KIB a bezpečnosti ISVS v SR

(monitorovanie a vyhodnocovanie bezpečnostných incidentov, inventarizácia odborných kapacít, možných zdrojov, analytická činnosť)

Vybudovanie kompetenčného centra KIB vo verejnej správe,

ktoré by na centrálnej úrovni zabezpečovalo riadenie KIB vo verejnej správe, technickú podporu pre špecializované činnosti v oblasti informačnej bezpečnosti a kontrolné mechanizmy na zabezpečovanie adekvátnej úrovne bezpečnosti IS VS

Štefánikova 15, 011 05 Bratislava
+ 421 2 2092 8018, martin.florian@mirri.gov.sk