

ITAPA | 16. 06. 2022

Vývoj a iniciatívy v kybernetickej bezpečnosti vo verejnom sektore

Martin Florián, PhD.

generálny riaditeľ sekcie kybernetickej bezpečnosti



Obsah

- 1 **Súčasný stav kybernetickej a informačnej bezpečnosti (KIB) vo verejnej správe (VS)**
- 2 **Vývoj a zlepšenia v riadení KIB vo VS za posledné 2 roky**
- 3 **Trendy v kybernetickej bezpečnosti**
- 4 **Iniciatívy v kybernetickej bezpečnosti vo VS**
- 5 **Plánované reformy pre kybernetickú bezpečnosť vo VS**
- 6 **Diskusia**

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

Hlavná výzva KIB vo VS
sú ľudia – ich **nedostatočné**
KIB povedomie
a stále **málo spôsobilých ľudí**
(Brainware)

Stav kybernetickej bezpečnosti vo VS sa postupne zlepšuje, ale stále nie je ideálny

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



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

Postupne zlepšujeme
riadenie KIB vo VS

Pozitívne zmeny pre riadenie KIB vo VS :

- **Technické a personálne posilnenie SKB** v kľúčových spôsobilostiach
- **Implementácia NSRIKBVVS a design spoločného SOC (Security Operation Center) pre VJ CSIRT a NASES**
- **Horizontálna dopytová výzva pre zlepšenie governance KIB vo VS**
- Zvyšovanie úrovne bezpečnosti v kybernetickom priestore VS prostredníctvom **dobudovania 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 „**templetov**“ a **šablón** pre OVM v zmysle vyhlášky 179/2020
- **Príprava KIB reforiem v POO** (Plán obnovy a odolnosti)
- Participujeme na realizácii Národnej stratégie kybernetickej bezpečnosti (schválená vládou SR 7. januára 2021) a na implementácii Akčného plánu NSKB



Trendy kybernetických útokov a riadenia KIB

Najviac sa pri útokoch stále používa phishing a sociálne inžinierstvo, ale prudko narastajú ransom-ware útoky

Menia sa „patterny“ a vzorce kybernetických útokov aj hrozieb.

- Informačné systémy sú stále najviac ohrozované cez **Phishing** a **Sociálne inžinierstvo**
- Posledné 2 roky prudko narástli **Ransom-ware** incidenty a hrozby
- **Cloud Security** narastá na strategickej dôležitosti
- Rýchly nástup **Umelej inteligencie (AI)** a **Dátovej Analytiky (D&A)**
- 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



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

Plánované KIB reformy 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)



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.**



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

Stratégia riadenia KIB vo VS
je premietnutá do
Akčného plánu NSKB

Konceptné ciele pre KIB vo VS :

- Posilnenie **preventívnych** riešení a lepšia **analýza** KIB relevantných **dát**
- Zvyšovanie úrovne bezpečnosti v kybernetickom priestore VS prostredníctvom dobudovania 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.



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.



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.



Princípy pre riadenie kybernetickej bezpečnosti vo verejnej správe



3. Zabezpečenie kvality a maximalizácia BCR

- 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 **zžitkovanie potenciálu** implementovaných riešení a systémov.



Princípy pre riadenie kybernetickej bezpečnosti vo verejnej správe



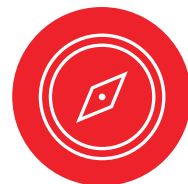
4. Viac modularity a fázovania vo veľkých projektoch

- 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.





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 alebo technológií
- Je dôležité **monitorovať objektívne trendy** a zapájať viac **meranie** a objektívnu **kvantifikáciu** pre prioritizáciu aj pre lepšie rozhodovanie.





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.





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.**





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.



DISKUSIA



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

www.mirri.gov.sk

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

ĎAKUJEME!

www.mirri.gov.sk



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

