Budovanie bezpečného štátu
(Čo máme za sebou a čo nás čaká ďalej?)

Rastislav Janota
riaditeľ

SK NBÚ CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Téma kybernetickej bezpečnosti sa týka každého.

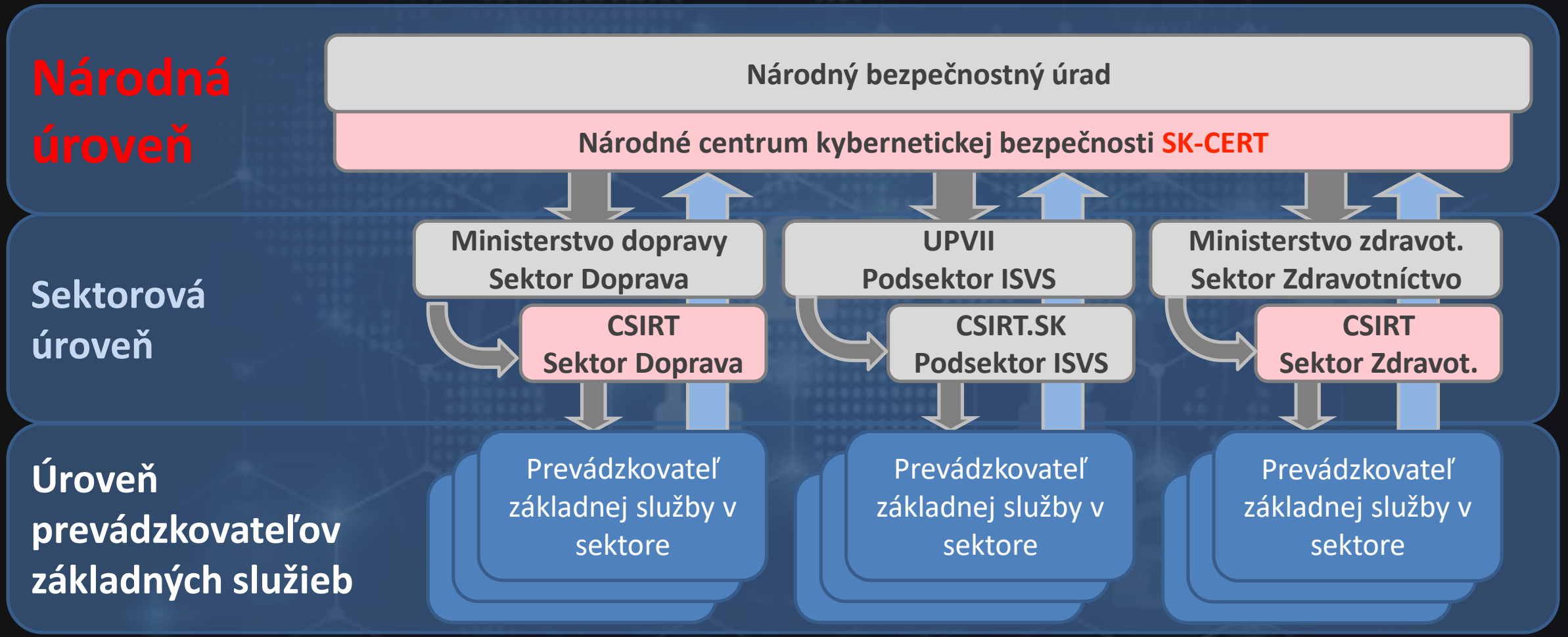
Každý je zodpovedný za svoje dáta, služby, zariadenia.

KDE SME DNES (I) - LEGISLATÍVA

- Zákon o kybernetickej bezpečnosti 69/2018 Zz.
  - Vyhláška 164/2018, ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
  - Vyhláška 165/2018, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
  - Vyhláška 166/2018 o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
  - Vyhláška 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

- Pripravovaná legislatíva
  - Vyhláška o pravidlách a rozsahu auditu kybernetickej bezpečnosti a a podrobnostiach o akreditovaní orcgánov posudzovania zhody
  - Vyhláška o bezpečnostných štandardoch a znalostných štandardoch

KDE SME DNES (II) - ZÁKLADNÉ ROLE



NATIONAL SECURITY AUTHORITY

KDE SME DNES (III) – PREVÁDZKA

- **Národné centrum kybernetickej bezpečnosti SK-CERT**
- Sektorový CSIRT.SK
- Sektorový CSIRT.MIL.SK
- GOV CERT SK

- **CSIRTy na Slovensku**
  - FIRST
    - 2 CSIRTY sú členmi
  - Trusted Introducer
    - 1 CSIRT pred ukončením certifikácie
    - 5 CSIRTov na úrovni „akreditovaný CSIRT“
    - 5 CSIRTov na úrovni „listed“

KDE SÚ SLABÉ MIESTA

- Nedostatok kvalifikovaných odborníkov
- Školský systém nepripravuje študentov v oblasti bezpečnosti
  - Risk manažéri, bezpečnostní IT špecialisti, programátori

- Slabá štandardizácia
- Nezáujem výrobcov o bezpečné HW produkty – narastá objem zraniteľností
- Bezpečnostne slabé architektúry a SW riešenia

- Minimálne bezpečnostné požiadavky nie sú dostatočné na bezpečný štát
- Nezáujem organizácii a firiem správať sa bezpečne
- Bezpečnosť nie je súčasť core business aktivít

- Slabá schopnosť štátu vyšetrovať kyberkriminalitu

ČO NÁS ČAKÁ

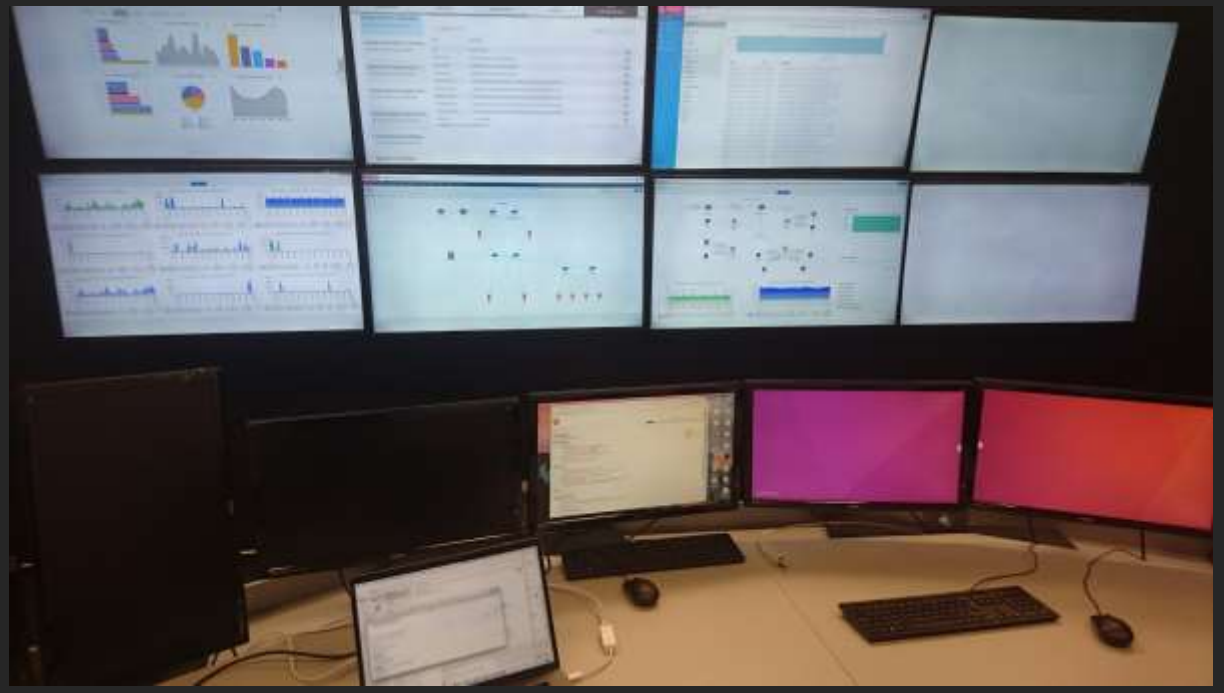
- Stratégia
  - Príprava novej Stratégie kybernetickej bezpečnosti SR na roky 2020 až 2025
- Legislatíva
  - Príprava novelizácie smernice NIS (pracovný názov NIS 2.0)
  - Nová telekomunikačná legislatíva
- Implementácia legislatívy
  - Priebežné určovanie ďalších základných služieb a ich prevádzkovateľov
  - Termíny na dosiahnutie súladu so zákonom o kybernetickej bezpečnosti
  - Začiatok pravidelného auditovania prevádzkovateľov základných služieb

- Nová realita
  - Zvyšovanie počtu aj sofistikovanosti útokov
  - Viac útokov zameraných na kradnutie osobných údajov rôzneho typuy
  - Zvyšovanie počtu cielených útokov na kritickú infraštruktúru
  - Zvyšovanie počtu cielených útokov na vládne systémy

AKO TEDA ĎALEJ?

- Podpora vzdelávania
  - Odborníci z praxe musia pomôcť školám vytvoriť vzdelávacie programy a učiť
  - Medzinárodná spolupráca s krajinami, kde je kybervzdelávanie na vyššej úrovni
- Implementačná podpora
  - Zdieľanie informácií, skúseností a best practice
- Znižovanie rizík
  - Awareness na všetkých úrovniach – od základných škôl až po seniorov
  - Vytvárať minimálne požiadavky prispôsobené jednotlivým sektorom
  - Úprava legislatívy pre zodpovedné oznamovanie zraniteľností (ochrana zdroja, povinnosti pre výrobcu)
- Zlepšovanie vymáhateľnosti
  - Úprava legislatívy pre uľahčenie vyšetrovania
- Detekcia
  - Zlepšovanie schopnosti detekcie udalostí na internete
  - Korelácia incidentov naprieč organizáciami a sektormi
  - Vytvorenie obranného mechanizmu proti dezinformáciám a hybridným hrozbám

NATIONAL SECURITY AUTHORITY



THANK YOU
ĎAKUJEM

rastislav.janota@nbu.gov.sk

SK CERT

NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI