Zákon o Kybernetickej bezpečnosti

Praktické otázky, implementácia a SK-CERT

Rastislav Janota
Riaditeľ
Národná jednotka SK-CERT

KOHO SA TÝKA KB?

Koho sa týka kybernetická a informačná bezpečnosť?

NÁS VŠETKÝCH!!!

Veď každý je zodpovedný za svoje vlastné dáta.

POVINNOSTI ZO ZÁKONA O KB (PZS)

- Riešiť kybernetický bezpečnostný incident,
- **Bezodkladne hlásiť závažný kybernetický bezpečnostný incident**,
- **Spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu** a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,
- V čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,

HLÁSENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

SK NBÚ CERT

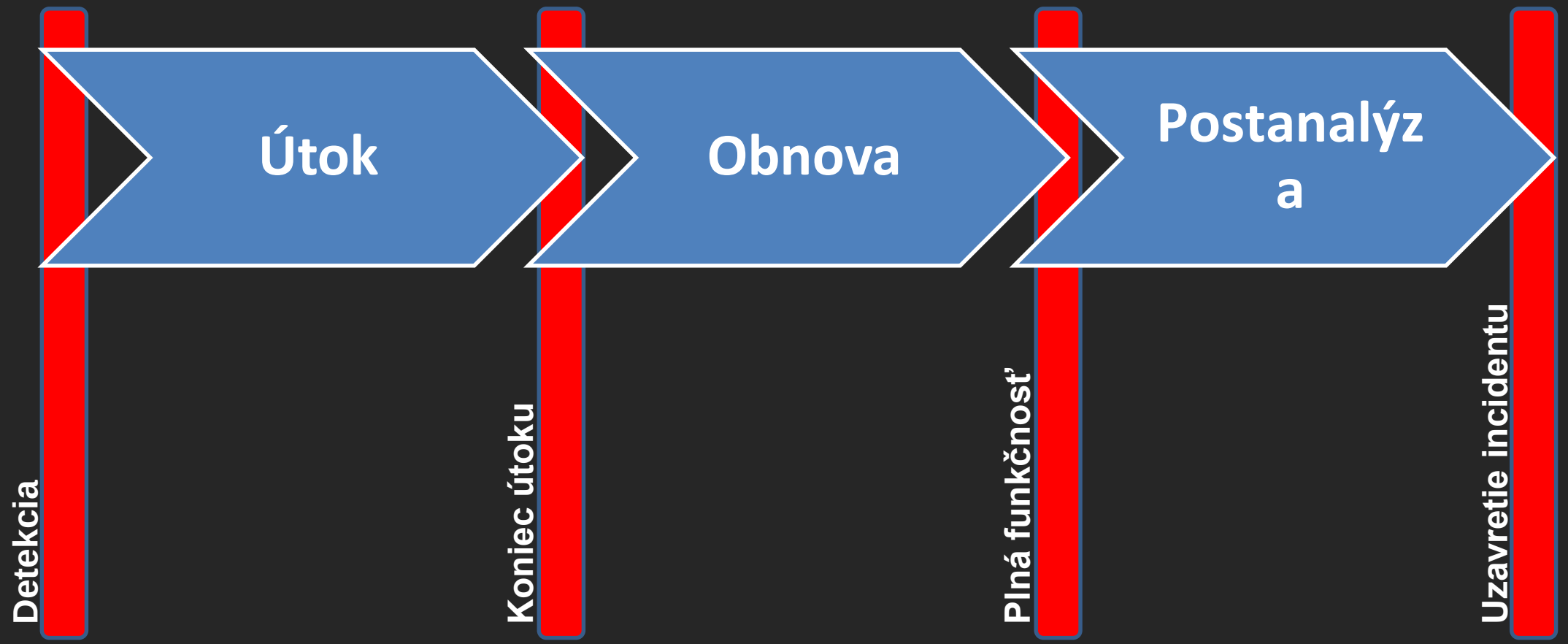
Umožňuje úradu

- Mať prehľad o stave kybernetickej bezpečnosti v SR v reálnom čase
- Získať informácie a skúsenosti zo zahraničia o konkrétnom incidente (ak existujú)
- Odporúčať efektívne spôsoby riešenia daného problému
- Na požiadanie subjektu efektívne asistovať/pomôcť pri riešení incidentu
- Varovať iné relevantné SR subjekty pred podobným problémom
- Rozširovať bázu vedomostí a pripravovať efektívne odporúčania v preventívnej oblasti tak, aby sa minimalizovalo riziko vzniku podobných incidentov v budúcnosti
- Aktualizovať vzdelávacie postupy a obsah na adresovanie potrieb na riešenie podobných incidentov v budúcnosti

- *Pre dosiahnutie týchto cieľov je nevyhnutná spolupráca (a informovanie úradu) od vzniku udalosti až po uzatvorenie incidentu*
- *Dôležitá je atmosféra dôvery*

HLÁSENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

SK NBÚ CERT



HLÁSENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

SK NBÚ CERT

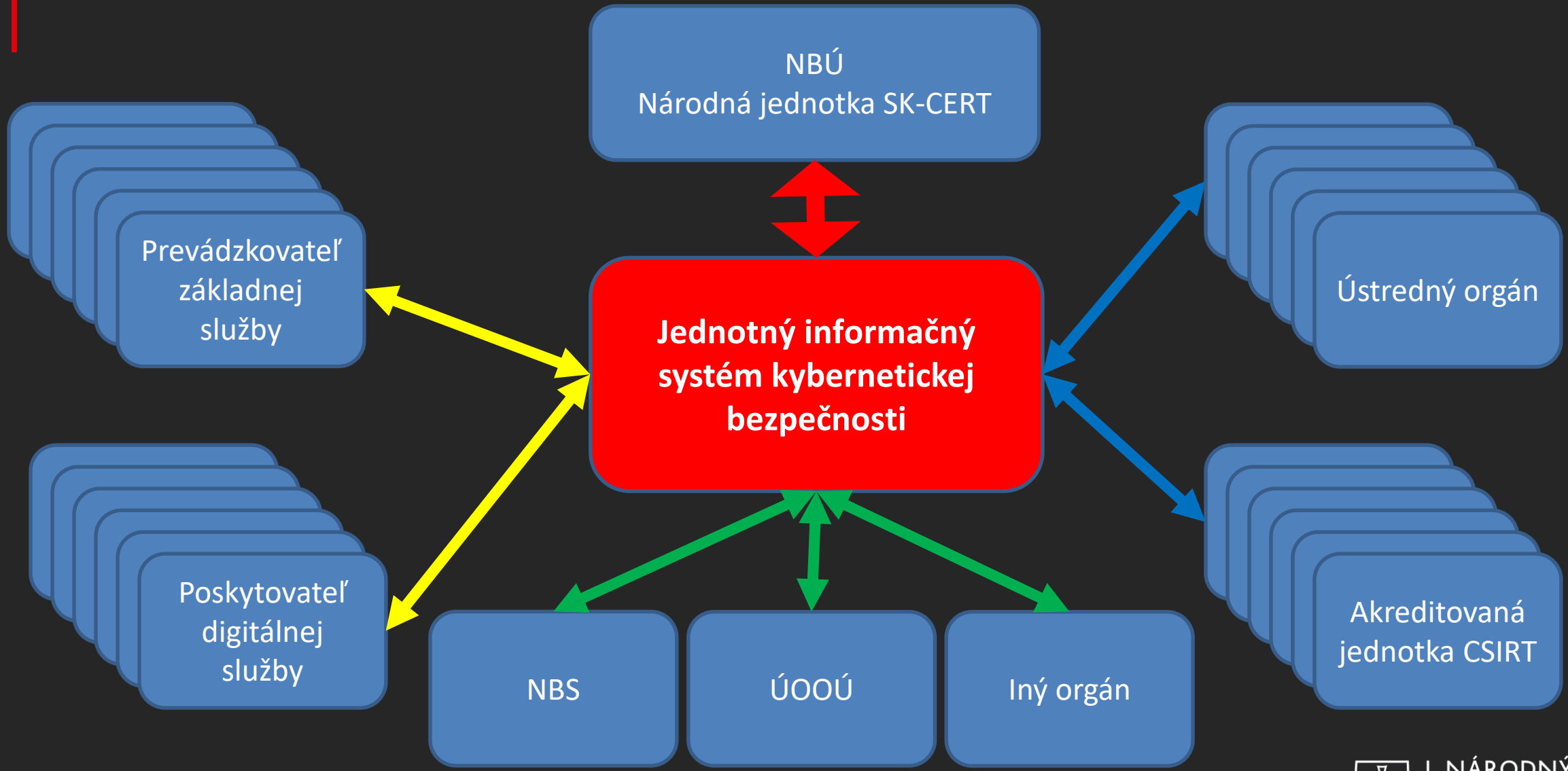
Spôsoby reportingu

- Reportovací formulár na webe Národnej jednotky SK-CERT.SK
- API rozhranie (JSON)
- Zmluvný reporting
    - § 24 Hlásenie kybernetických bezpečnostných incidentov prevádzkovateľom základnej služby ods. 6) ZoKB
      Na účely hlásenia kybernetických bezpečnostných incidentov a zaistenia funkcionality jednotného informačného systému kybernetickej bezpečnosti môže úrad namiesto postupu uvedeného v § 8 ods. 6 uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s prevádzkovateľom základnej služby.
- Povinný obsah reportingu je predmetom vyhlášky NBU
    - Identifikačné kritériá pre jednotlivé kategórie kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov

- Hlásenie sa vykonáva **VÝHRADNE** prostredníctvom jednotného informačného systému kybernetickej bezpečnosti (§ 24 ods. 4)

HLÁSENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

SK NBÚ CERT



RIEŠENIE KYBERNETICKÝCH INCIDENTOV (§27)

SK NBÚ CERT

- V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby môže úrad
  a) vyhlásiť výstrahu a varovanie pred závažným kybernetickým bezpečnostným incidentom,
  b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,
  c) uložiť povinnosť vykonať reaktívne opatrenie,
  d) požadovať návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenie“).
- Povinnosť riešiť kybernetický bezpečnostný incident ukladá úrad rozhodnutím tomu, kto plní úlohy jednotky CSIRT, prevádzkovateľovi základnej služby a poskytovateľovi digitálnej služby
- Reaktívne opatrenie je priama odpoveď na závažný kybernetický bezpečnostný incident
- Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím prevádzkovateľovi základnej služby alebo poskytovateľovi digitálnej služby, ktorí sú pri riešení závažného kybernetického bezpečnostného incidentu nečinní, alebo ak riešenie závažného kybernetického bezpečnostného incidentu je zjavne neúspešné.

SLUŽBY SK-CERT

- Proaktívne služby
  - Oznámenia a upozornenia
    - Systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike, vyhľadáva
    - Vytvára adresné upozornenia spolu s bezpečnostným odporúčaním firmám a jednotlivcom u ktorých boli zistené zneužiteľné konfigurácie
  - Služby prevencie a detekcie narušenia
    - Implementácia honeypotov, SPAM pascí, senzorov na detekciu šírenia nežiadúcich aktivít v lokálnych sieťach
    - Automatické sledovanie a vyhodnocovanie takýchto informácii a vytváranie upozornení pre zákazníka
  - Distribúcia bezpečnostne relevantných informácii, bulletiny a varovania
    - Aktívne vyhľadávanie informácii o hrozbách a zraniteľnostiach z medzinárodných zdrojov, analýza kritickosti, vytváranie odporučených postupov na ochranu pred danou hrozbou/zraniteľnosťou a distribúcia takýchto informácii prostredníctvom týždňových bezpečnostných bulletinov alebo kritických varovaní
  - Zdieľanie informácií o hrozbách, zraniteľnostiach a iných informácií
    - Prevádzka platformy na obojsmerné zdieľanie informácii o zraniteľnostiach, indikátoroch kompromitácie, vzoriek škodlivého kódu a pod.

SLUŽBY SK-CERT

- Reaktívne služby
  - Služby prevádzkového a bezpečnostného monitoringu (SOC)
    - Automatický zber, sledovanie a vyhodnocovanie logov zo zariadení klienta
  - Manažment a riešenie incidentov (incident handling)
    - Asistencia pri riešení incidentu, zdieľanie postupov a informácii potrebných na efektívne vyriešenie incidentu
  - Forenzná analýza
    - Skúmanie potenciálne kompromitovaných zariadení (počítače, servery, sieťové zariadenia, mobilné zariadenia a pod.) a vyhľadávanie dôkazov o ich napadnutí
  - Analýza artefaktov a zraniteľností
    - Analýza vzoriek škodlivého kódu, hľadanie spôsobov obrany, resp vytváranie znalostnej databázy o spôsoboch útoku a formách ochrany pred danými útokmi
    - Analýza zariadení a aplikácii, hľadanie dier, zraniteľností a postupov, vedúcich ku kompromitácii zariadení a aplikácii

SLUŽBY SK-CERT A NBÚ

- Služby kvality zabezpečenia (ostatné služby)
  - Budovanie povedomia
    - Zabezpečuje tréningové možnosti pre zvyšovanie bezpečnostného povedomia žiakov, študentov a zamestnancov firiem či štátu v oblasti rizík na internete
  - Vzdelávanie a tréning
    - Zabezpečuje tréningové stredisko a tréningy pre cielené zvyšovanie kvalifikácie u pracovníkov v obore IT, bezpečnostných špecialistov a vedúcich pracovníkov
  - Certifikácia produktov a služieb
    - Na žiadosť právnických osôb vykonáva certifikáciu prostriedkov podľa medzinárodných a národných štandardov
  - Bezpečnostné poradenstvo
    - Na požiadanie vykonáva poradenstvo pri návrhu a implementácii bezpečnostných technológii, informačných systémov a sietí najmä pre orgány verejnej moci a prvky kritickej infraštruktúry

ĎAKUJEM ZA POZORNOSŤ

SK NBÚ CERT

rastislav.janota@nbu.gov.sk