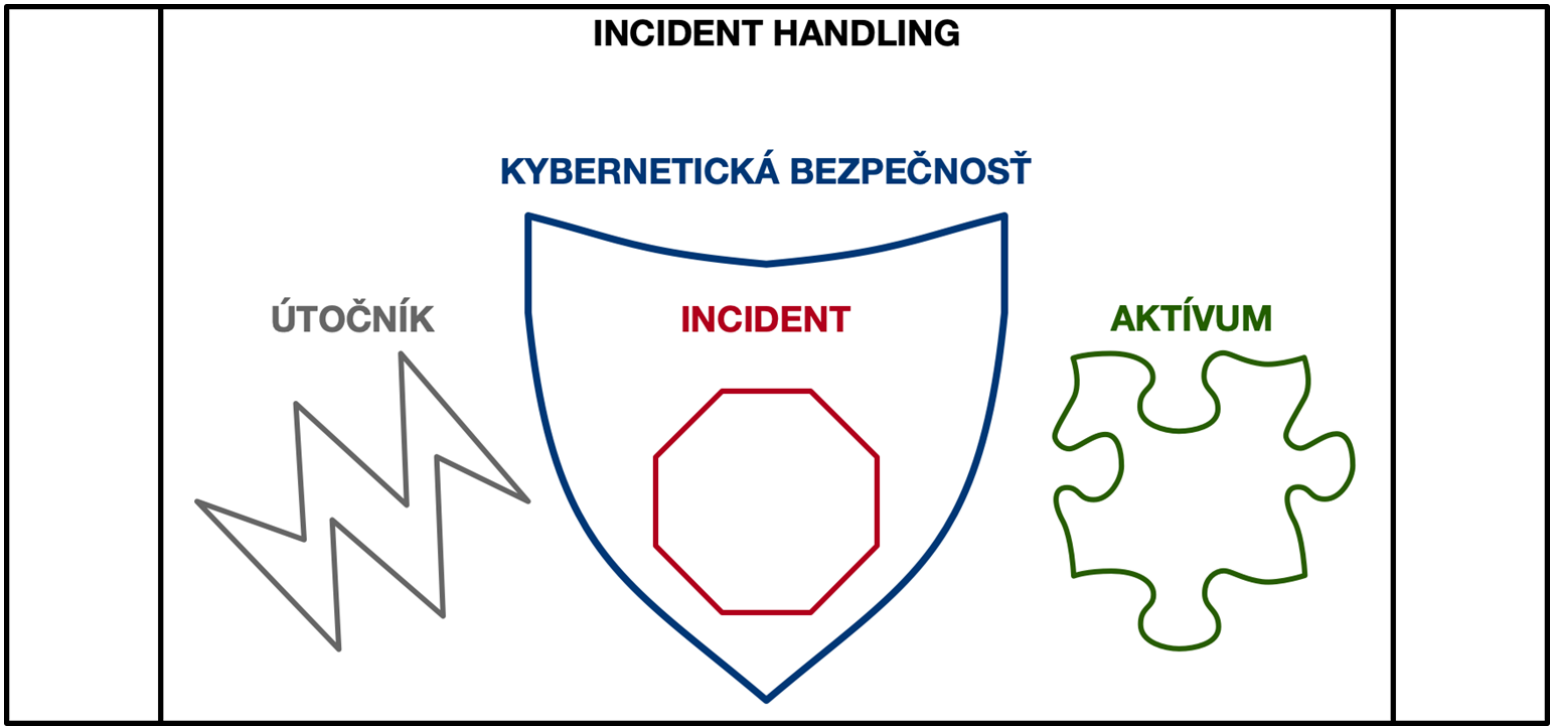
Aktuálne hrozby, incidenty a využitie JISKB pri ich riešení

Ján Doboš
jan.dobos@nbu.gov.sk

Aktíva, hrozby, incidenty, …



HROZBY v kybernetickom priestore SR 2026

- predikcie, ktoré sa na(ne)šťastie napĺňajú…

https://www.nbu.gov.sk/hrozby-v-kybernetickom-priestore-2026/

I. Phishing a sociálne inžinierstvo

- rôzne formy a scenáre
- rovnaké ciele

- phishing-as-a-service

- obchádzanie zaužívaných bezpečnostných mechanizmov

I. Phishing a sociálne inžinierstvo + AI ako akcelerátor

- zvyšovanie dôveryhodnosti obsahu
- tvorba cieleného až personalizovaného obsahu

- vývoj nových metód a frameworkov

- od človeka používajúceho AI k autonómnym agentovým swarmom

II. Zraniteľné systémy

- definícia zraniteľnosti

“Úmyselná alebo neúmyselná chyba HW, SW alebo P ktorá môže byť zneužitá a viesť k vzniku kybernetického bezpečnostného incidentu” (CVE)

II. Zraniteľné systémy

- rozšírená definícia zraniteľnosti

“Nesprávna konfigurácia alebo nedostatočné zabezpečenie zariadenia alebo systému”

II. Zraniteľné systémy

- ešte viac rozšírená definícia zraniteľnosti

“Zariadenia s ukončenou podporou”

“AI ako (ne)predvídateľná entita v organizácii”

II. Zraniteľné systémy + AI ako akcelerátor

- identifikácia, oprava a zneužitie
- od človeka používajúceho AI k autonómnym agentovým swarmom

III. Úniky dát

- prihlasovacie údaje a kryptografický materiál
- citlivé údaje
  - osobné, finančné, zdravotné, biometrické, behaviorálne, …

- zraniteľnosť, chybná konfigurácia, phishing, malware, ransomware, insider

III. Úniky dát

- zverejnenie, predaj alebo priame zneužitie
- príprava cieleného útoku, získanie prístupu, vydieranie
- kľúčový pilier kybernetickej kriminality, ktorý mení celý ekosystém útočníkov
  - vďaka IAB sa skupiny môžu zamerať na plnenie primárneho cieľa

IV. Útoky na dodávateľské reťazce

- outsourcing business procesov, IKT, rozšírenia softwaru, knižnice, závislosti, vzdialený prístup dodávateľov, …

- musíme vedieť čo chránime, čo nám hrozí a čo je ohrozené a ako sa chrániť
  - manažment aktív + attack surface
  - manažment zraniteľností + CTI
  - manažment aktualizácií, bezpečnostný dohľad

https://www.sk-cert.sk/sk/utoky-cieliace-na-vyvojarov-softveru

V. AI ako príležitosť, riziko aj nástroj zmiernenia rizík

- zber, analýza, syntéza, vývoj, módny poradca, kamarát, autonómna sila

- ako ju správne riadiť a zabezpečiť, aby sa nestala neviditeľným vnútorným nepriateľom
  - vidí hlbšie do infraštruktúry, vie viac a dokáže robiť stále zložitejšie úkony

- niektoré typy útokov pravdepodobne nebude možné úplne mitigovať

V. AI ako príležitosť, riziko aj nástroj zmiernenia rizík

- ruku na srdce…

- … AI ako nevyhnutnosť

- … AI ako sila vplývajúca na vývoj ďalších generácií

VI. Dôveruj, ale preveruj... A VŠETKO

- článok, post na sociálnej sieti
  - deepfake, syntetické profily
  - dezinformácie, šírenie naratívov
- výsledok vyhľadávania cez vyhľadávač alebo AI
  - popularita produktu alebo služby
  - linka na stiahnutie softwaru
  - návod na riešenie problému
- SEO poisoning, platená reklama, manipulácia AI, likeovanie a recenzie

Dokonalá bezpečnosť neexistuje

Incident nie je zlyhaním. Zlyhaním je nepripravenosť…

Poznať svoje práva a povinnosti a mať pripravené, funkčné a otestované postupy:		
PRED	**POČAS**	**PO**
- Správa aktív - Riadenie rizík - Procesy riešenia incidentov - Business continuity plán - Technické opatrenia - Povedomie o hrozbách - Vzdelávanie	- Zamedzenie šírenia - Plná odozva na incident - Vykonanie neopakovateľných úkonov - Analýza útoku a plán obnovy - Hlbšia technická analýza - Bezpečná obnova - Komunikačná a právna stránka incidentu - Hlásenia	- Zhodnotenie celého priebehu riešenia incidentu - Identifikácia problémov a nedostatkov - Aktualizácia procesov - Odstránenie nedostatkov

https://cri.sk-cert.sk

Ako byť pripravený a na nič nezabudnúť?

Audit a samohodnotenie:

- Odhaľuje slabé miesta
- Preveruje procesy
- Znižuje riziko dopadu incidentov
- Pomáha plniť povinnosti

“Nevymýšľajme, čo už bolo vymyslené”

INCIDENTY v kybernetickom priestore SR (ZOKB)

	2021	2022	2023	2024
Dobrovoľné	878	1135	948	1155
Kategória I	22	20	19	17
Kategória II	11	8	4	6
Kategória III	1	7	3	1
CELKOM	**912**	**1 170**	**974**	**1179**

	2025
KBI - Dobrovoľné	1575
KBI - Povinné	75
Hrozba	14
Udalosť	19
Zraniteľnosť	6
CELKOM	**1689**

Nebojme sa incidenty hlásiť !!!

INCIDENTY v kybernetickom priestore SR (TECH)

2023		2024		2025	
Získavanie informácií	**611**	**Získavanie informácií**	**660**	**Získavanie informácií**	**1067**
Nedostupnosť	88	Prienik do systému	112	Prienik do systému	126
Prienik do systému	64	Nedostupnosť	82	Nedostupnosť	106
Škodlivý kód	49	Pokus o prienik	80	**Zraniteľnosť**	**89**
Zraniteľnosť	**46**	**Zraniteľnosť**	**68**	Škodlivý kód	66
Ostatné	116	Ostatné	69	Ostatné	62
CELKOM	**974**	**CELKOM**	**1179**	**CELKOM**	**1689**

Vzdelávajme zamestnancov a dbajme o infraštruktúru !!!

Prečo hlásime?

- splnenie zákonnej povinnosti
- pomoc s riešením incidentu (rôzne formy participácie CSIRT jednotky)
- vyššie dobro a ochrana kybernetického priestoru SR

Ako hlásime? Čo produkujeme? Ako sa v tom nestratiť?

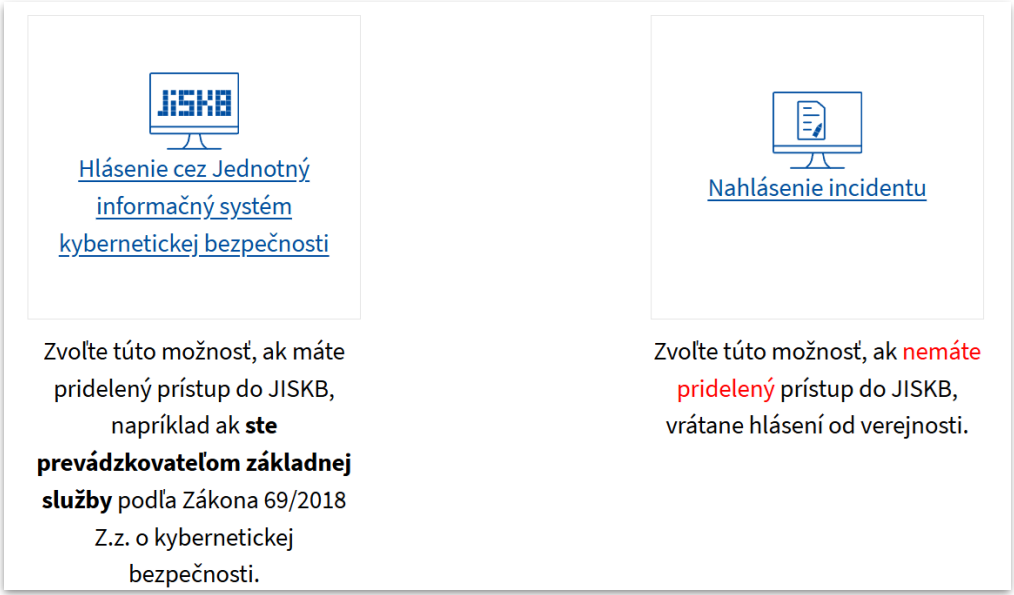
- štandardné komunikačné kanály
- špecializované technické prostriedky

- hlásenia rôznej formy, kvantity aj kvality (objektívne a subjektívne činitele)

- potreba štandardizácie a zjednotenia formátu hlásení

JISKB - Jednotný

- regulované subjekty (PZS, PKZS)
- neregulované subjekty, anonym

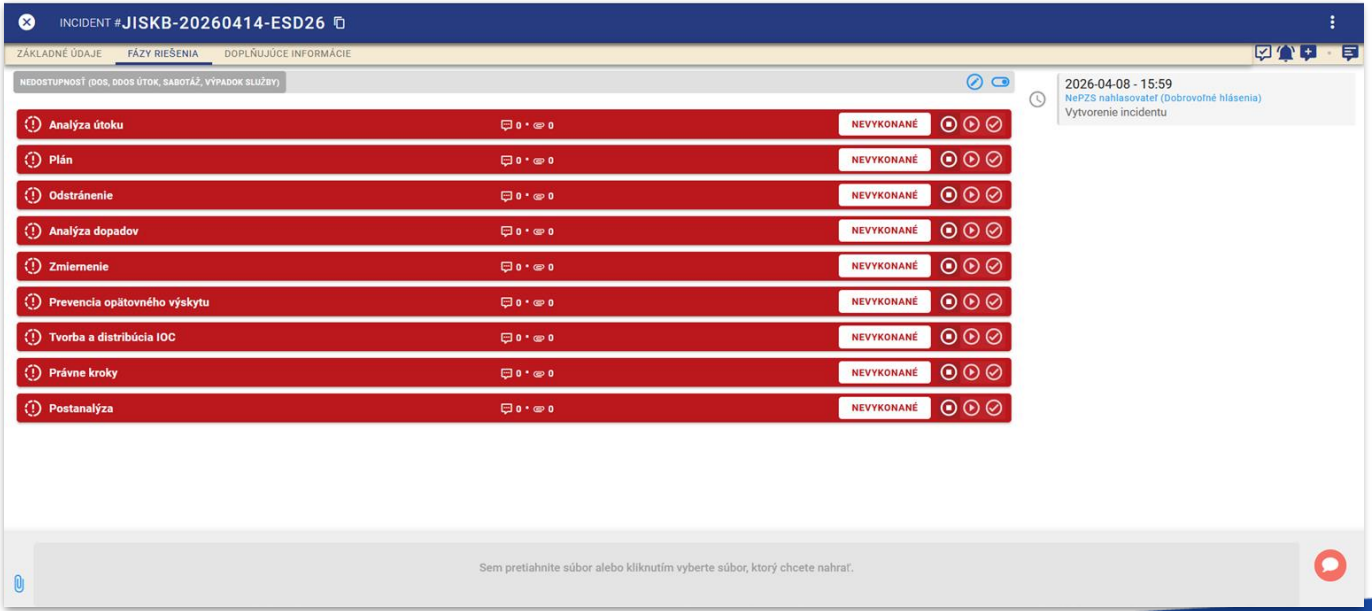


JISKB - Jednotný

- zastrešiť všetky náležitosti vyplývajúce zo zákona o kybernetickej bezpečnosti a vyhlášok

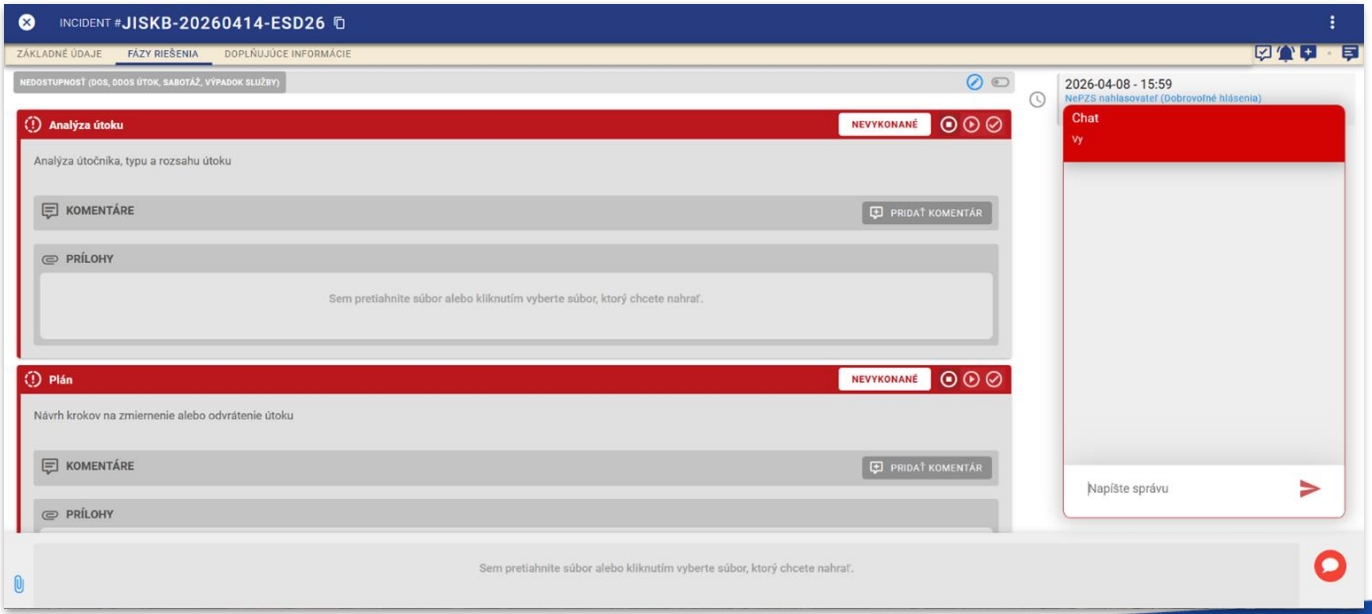
JISKB - Jednotný Informačný

- udržiavanie aktuálnych údajov
- prehľad o hláseniach a stave ich riešenia, komunikácia a koordinácia



JISKB - Jednotný Informačný

- udržiavanie aktuálnych údajov
- prehľad o hláseniach a stave ich riešenia, komunikácia a koordinácia



JISKB - Jednotný Informačný Systém

- “živý a rozvíjajúci sa tvor”

- zmeny v legislatíve
- typológia a fázy riešenia incidentu
- praktické skúsenosti a pripomienky

- moduly pre samohodnotenie a audit, zodpovedné oznamovanie zraniteľností

Používatelia → Spätná väzba → Rozvoj

Aktuálne hrozby, incidenty a využitie JISKB pri ich riešení

Ján Doboš
jan.dobos@nbu.gov.sk