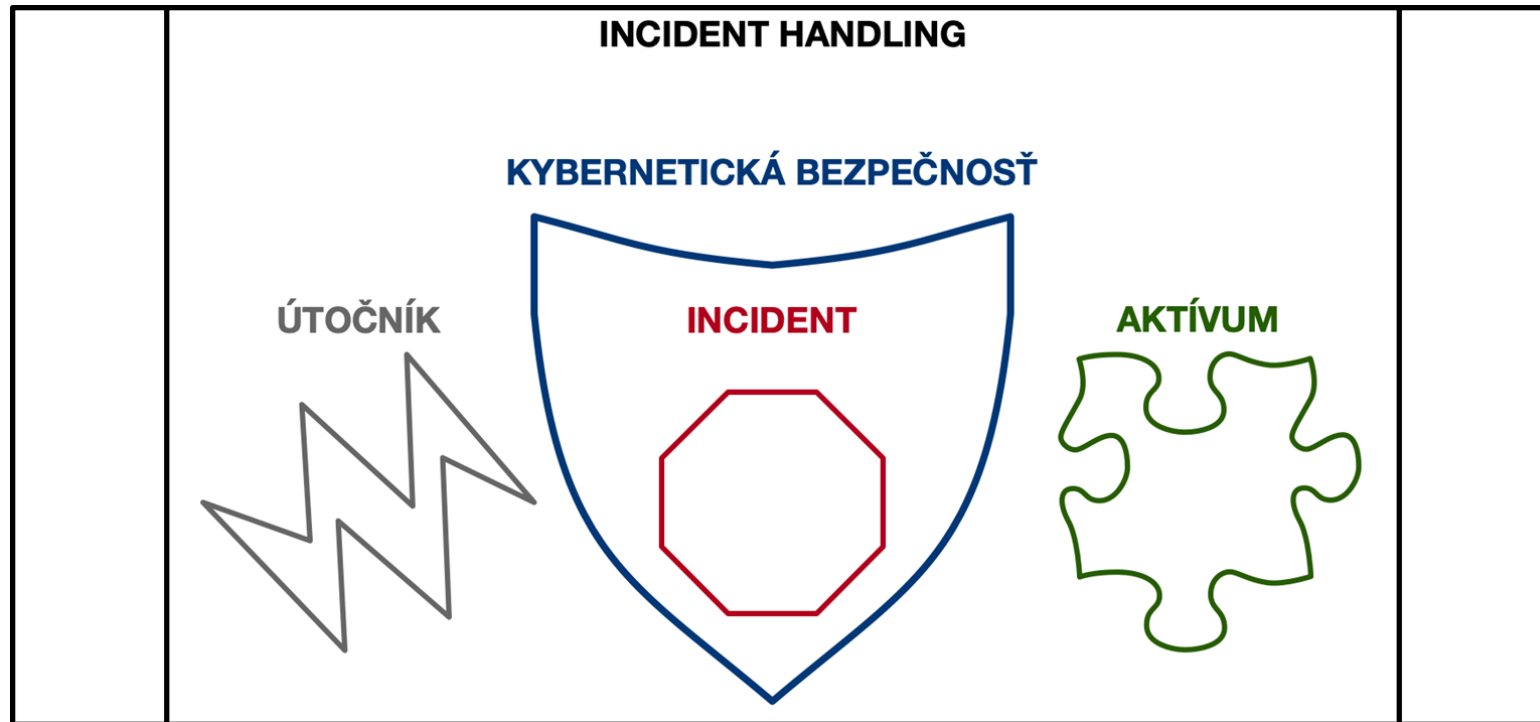




# Aktuálne hrozby, incidenty a využitie JISKB pri ich riešení

Ján Doboš  
[jan.dobos@nbu.gov.sk](mailto:jan.dobos@nbu.gov.sk)

# Aktíva, hrozby, incidenty, ...



# HROZBY v kybernetickom priestore SR 2026

- predikcie, ktoré sa na(ne)šťastie naplňajú...



<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 cieľeného 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, módnny 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
<ul style="list-style-type: none"> <li>- Správa aktív</li> <li>- Riadenie rizík</li> <li>- Procesy riešenia incidentov</li> <li>- Business continuity plán</li> <li>- Technické opatrenia</li> <li>- Povedomie o hrozbách</li> <li>- Vzdelávanie</li> </ul>	<ul style="list-style-type: none"> <li>- Zamedzenie šírenia</li> <li>- Plná odozva na incident</li> <li>- Vykonanie neopakovateľných úkonov</li> <li>- Analýza útoku a plán obnovy</li> <li>- Hlbšia technická analýza</li> <li>- Bezpečná obnova</li> <li>- Komunikačná a právna stránka incidentu</li> <li>- Hlásenia</li> </ul>	<ul style="list-style-type: none"> <li>- Zhodnotenie celého priebehu riešenia incidentu</li> <li>- Identifikácia problémov a nedostatkov</li> <li>- Aktualizácia procesov</li> <li>- Odstránenie nedostatkov</li> </ul>

<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
<b>CELKOM</b>	<b>912</b>	<b>1 170</b>	<b>974</b>	<b>1179</b>

	2025
KBI - Dobrovoľné	1575
KBI - Povinné	75
Hrozba	14
Udalosť	19
Zraniteľnosť	6
<b>CELKOM</b>	<b>1689</b>

**Nebojme sa incidenty hlásiť !!!**

# INCIDENTY v kybernetickom priestore SR (TECH)

2023		2024		2025	
Získavanie informácií	<b>611</b>	Získavanie informácií	<b>660</b>	Získavanie informácií	<b>1067</b>
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	<b>Zraniteľnosť</b>	<b>89</b>
<b>Zraniteľnosť</b>	<b>46</b>	<b>Zraniteľnosť</b>	<b>68</b>	Škodlivý kód	66
Ostatné	116	Ostatné	69	Ostatné	62
<b>CELKOM</b>	<b>974</b>	<b>CELKOM</b>	<b>1179</b>	<b>CELKOM</b>	<b>1689</b>

**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



[Hlásenie cez Jednotný  
informačný systém  
kybernetickej bezpečnosti](#)

Zvoľte túto možnosť, ak máte  
pridelený prístup do JISKB,  
napríklad ak **ste**  
**prevádzkovateľom základnej**  
**služby** podľa Zákona 69/2018  
Z.z. o kybernetickej  
bezpečnosti.



[Nahlásenie incidentu](#)

Zvoľte túto možnosť, ak **nemáte**  
**pridelený** prístup do JISKB,  
vrátane hlásení od verejnosti.

# JISKB - Jednotný

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



## Nahlásiť incident

Incident je udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov.



## Nahlásiť udalosť odvrátenú v poslednej chvíli

Udalosť odvrátená v poslednej chvíli, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo.



## Nahlásiť zraniteľnosť

Zraniteľnosť je akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou.



## Nahlásiť kybernetickú hrozbu

Kybernetická hrozba je každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby.

# JISKB - Jednotný Informačný

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

INCIDENT #JISKB-20260414-ESD26

ZÁKLADNÉ ÚDAJE FÁZY RIEŠENIA DOPLŇUJÚCE INFORMÁCIE

NEODSTUPNOSŤ (DOS, DOS ÚTOK, SABOTÁŽ, VÝPADOK SLUŽBY)

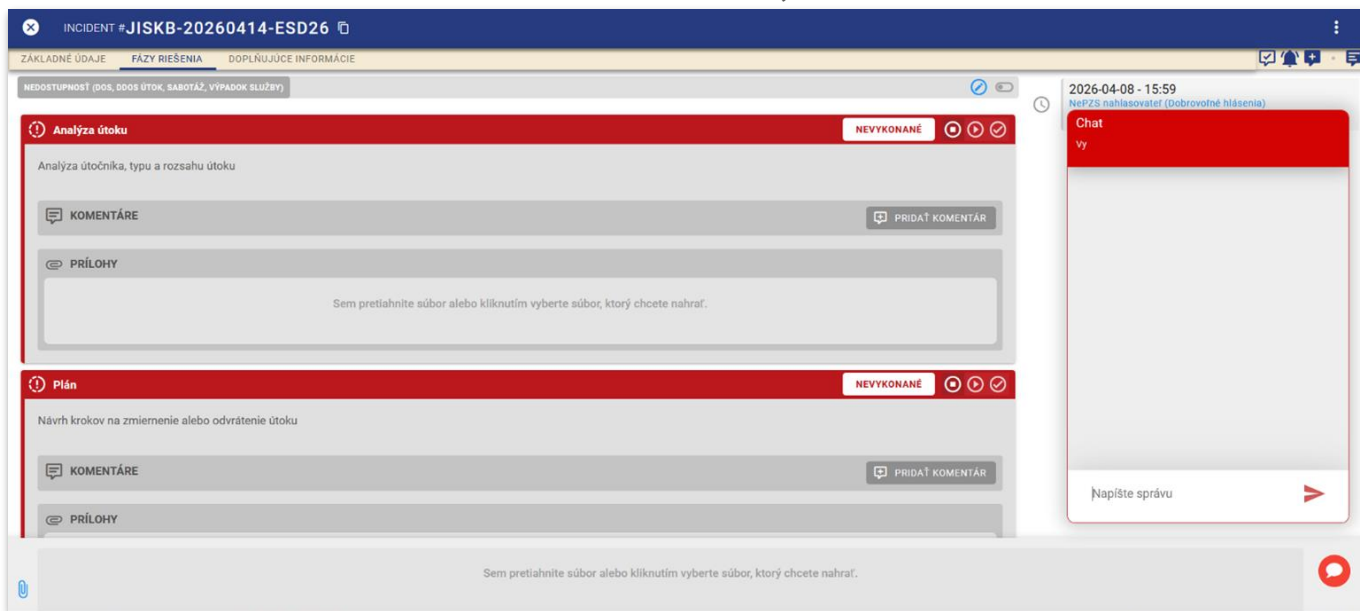
Úloha	Stav	Prístup
Analyza útoku	NEVYKONANÉ	🗨️ 📄 🔄
Plán	NEVYKONANÉ	🗨️ 📄 🔄
Odstránenie	NEVYKONANÉ	🗨️ 📄 🔄
Analyza dopadov	NEVYKONANÉ	🗨️ 📄 🔄
Zmlernenie	NEVYKONANÉ	🗨️ 📄 🔄
Prevenca opätovného výskytu	NEVYKONANÉ	🗨️ 📄 🔄
Tvorba a distribúcia IOC	NEVYKONANÉ	🗨️ 📄 🔄
Právne kroky	NEVYKONANÉ	🗨️ 📄 🔄
Postanalýza	NEVYKONANÉ	🗨️ 📄 🔄

2026-04-08 - 15:59  
NePZS nahlasovateľ (Dobrovoľné hlásenia)  
Vytvorenie incidentu

Sem pretiahnite súbor alebo kliknutím vyberte súbor, ktorý chcete nahráť.

# 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](mailto:jan.dobos@nbu.gov.sk)