Nové výzvy pro provozovatele kritických informačních systémů

Ing. Bohuslav Zůbek, CMICT

Samostatné oddělení kybernetické bezpečnosti

Ministerstvo vnitra

15. května 2025

Klasifikace: **Veřejné**, **TLP:GREEN**

Obsah

- Ministerstvo vnitra
- Vývoj kybernetických bezpečnostních událostí a incidentů, přehled za rok 2024
- Aktuální hrozby
- Zpracování informací v cloudu
- Ransomware iniciativa
- Umělá inteligence (AI) a budoucnost
- Budoucí vývoj – trendy

Ministerstvo vnitra

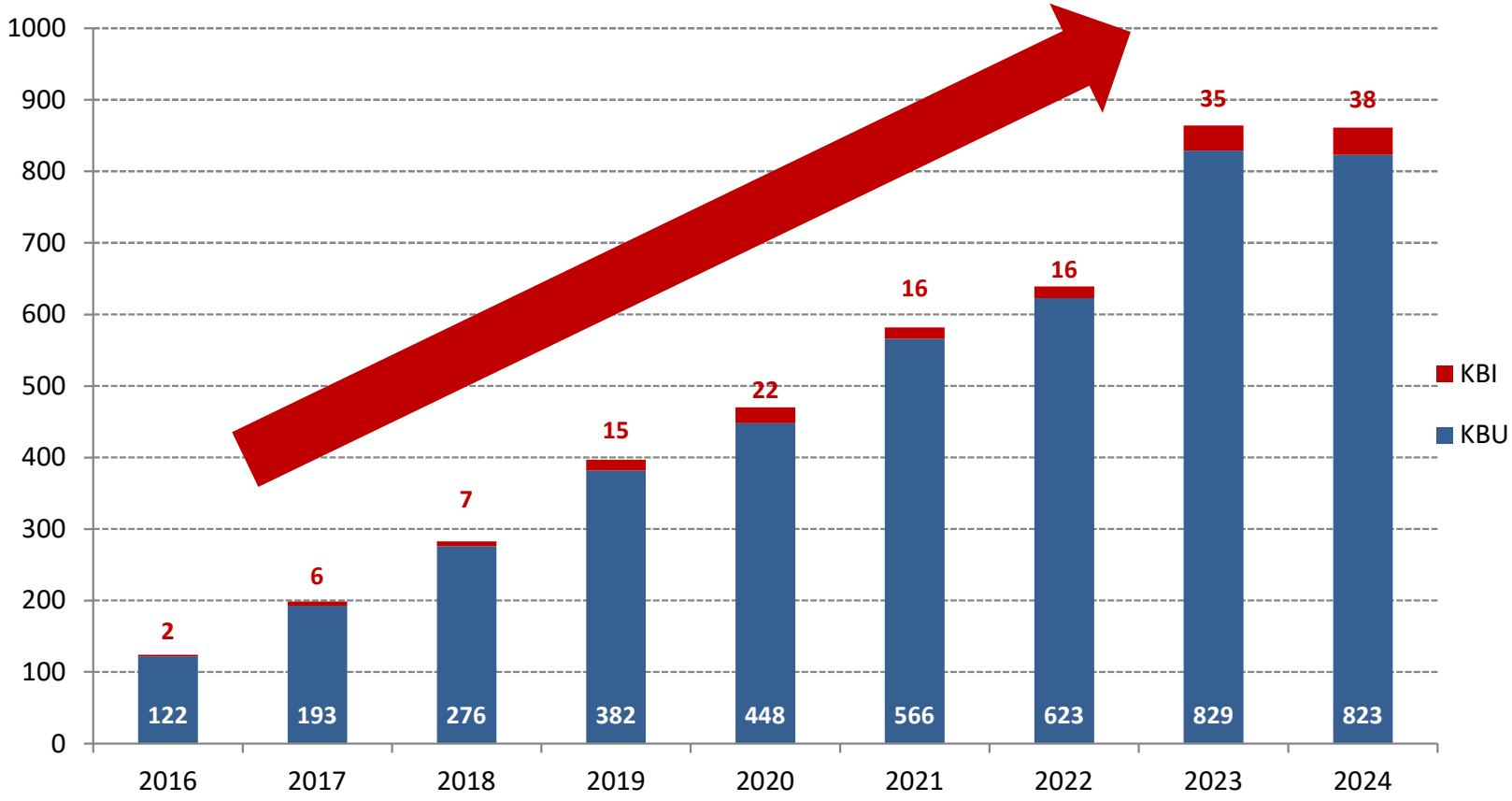
- **Ministerstvo vnitra** je ústředním orgánem státní správy pro vnitřní věci, zejména pro veřejný pořádek a další věci vnitřního pořádku a bezpečnosti.
- Zajišťuje komunikační sítě pro Policii ČR, složky integrovaného záchranného systému a územní orgány státní správy a provozuje informační systém pro nakládání s utajovanými informacemi mezi orgány veřejné moci.
- Plní koordinační úlohu pro komunikační technologie.
- Resort tvoří více než **50** organizací včetně krajských ředitelství Policie ČR a Hasičského záchranné sboru ČR.

Vývoj kybernetických bezpečnostních událostí a incidentů

Z celkového počtu 38 KBI a 823 KBU, které eviduje DCeGOV za rok 2024, připadalo na resort MV:

- **26 KBI** a
- **698 KBU**.

Přehled KBU a KBI v letech 2016-2024
(Celkem zaznamenáno DCeGOV)



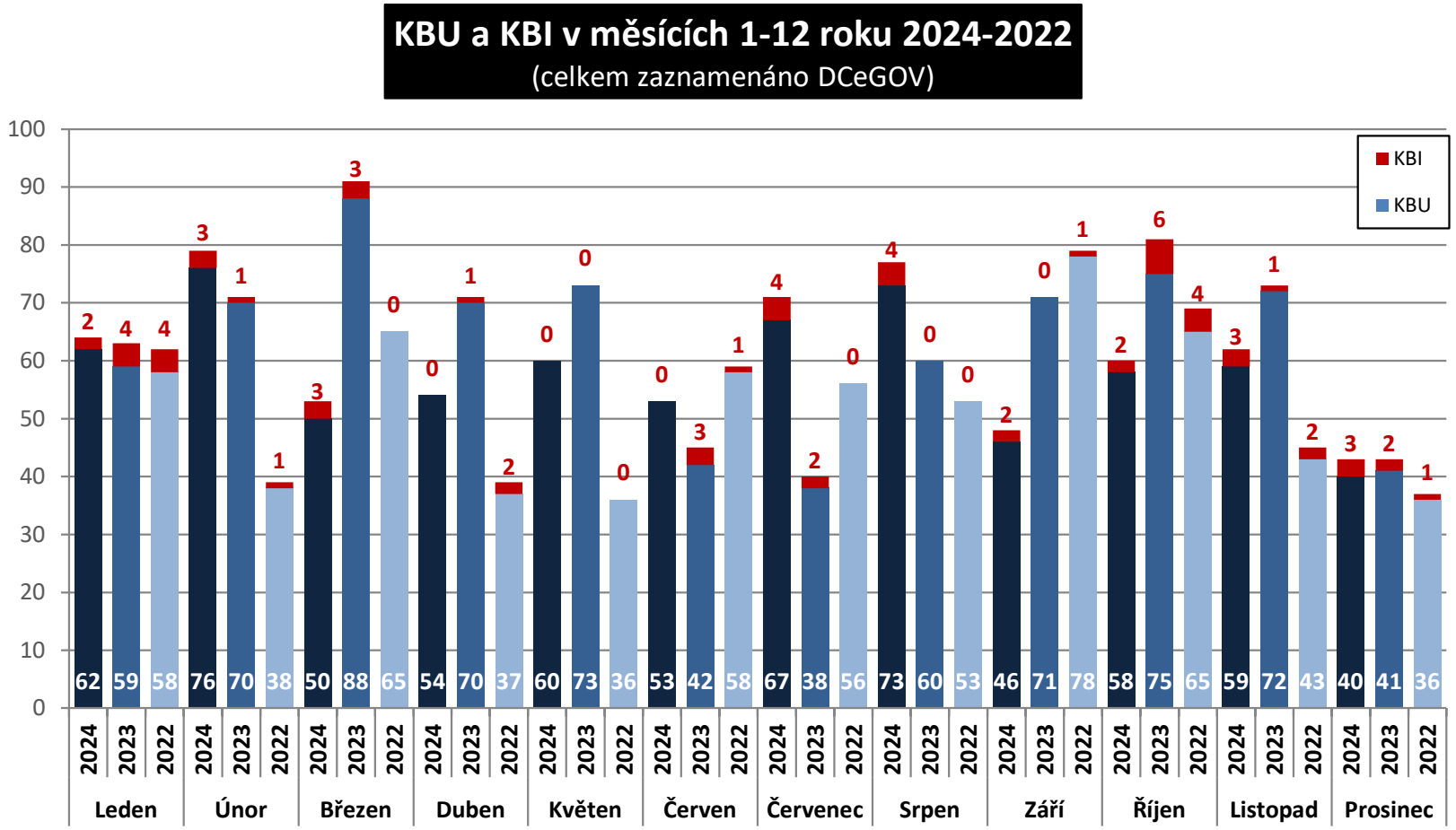
Přehled KBU a KBI za rok 2024

∑2024=861

∑2023=864

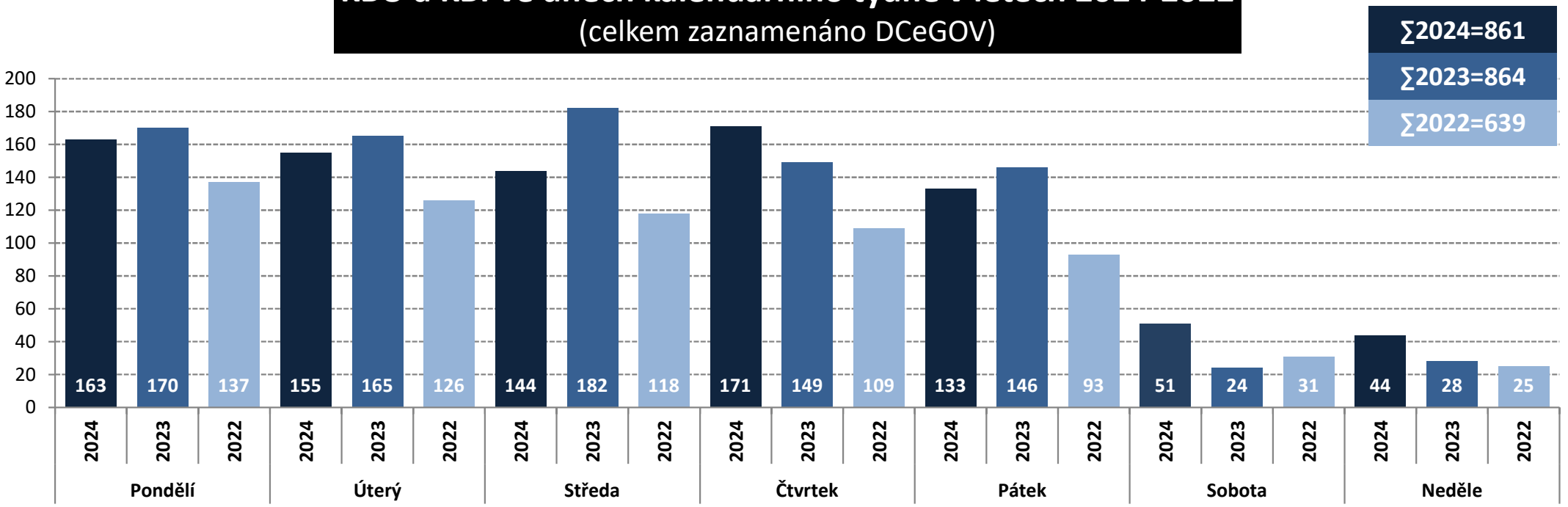
∑2022=639

- Celkový počet **kybernetických bezpečnostních událostí** zaznamenaných v DCeGOV se v roce 2024 proti roku 2023 poklesl o 0,7 % na **823**.
- Celkový počet **kybernetických bezpečnostních incidentů** se zvýšil o 8,6% na **38**.



Přehled KBU a KBI za rok 2024

KBU a KBI ve dnech kalendářního týdne v letech 2024-2022
(celkem zaznamenáno DCeGOV)



	2024	2023	2022
Největší počet KBU a KBI	Středa	Středa	Pondělí
Nejmenší počet KBU a KBI	Sobota	Sobota	Neděle

- Útoky typu DoS/DDoS (zahlcení webových portálů, služby DNS, . . .).
- Pokusy o zneužití zranitelností.
- Skenování sítě, získávání informací.
- Útoky hrubou silou (pokusy o prolomení přihlašovacích údajů).
- Útoky mířící přímo na uživatele (podvodné e-maily, volání, zprávy na WhatsApp . . .).
- Škodlivý kód vč. ransomware.

- Model nazvaný Cypre Language Model (CLM), který je speciálně navržen pro kybernetickou bezpečnosti. Model je zaměřen na ochranu národní kritické infrastruktury před sofistikovanými útoky.
- Klíčové vlastnosti CLM:
  - Prediktivní detekce hrozeb: CLM využívá umělou inteligenci k předvídání potenciálních kybernetických hrozeb dříve, než se stanou skutečnými útoky.
  - Automatizovaná analýza bezpečnosti: Model provádí automatizovanou analýzu bezpečnostních rizik a poskytuje v reálném čase obranné mechanismy k neutralizaci hrozeb.
  - Simulace reálných kybernetických útoků: CLM funguje jako obránce i útočník, což umožňuje simulovat skutečné kybernetické útoky a identifikovat zranitelnosti v systémech.
  - Nepřetržité monitorování sítí: Systém neustále monitoruje sítě, identifikuje potenciální narušení a neutralizuje rizika dříve, než se eskalují.
- Na základě poskytnutých konfiguračních souborů např. z routerů a jiných prvků umí CLM nakreslit mapu organizace a zároveň poskytnout doporučení na základě zjištěných rizik.

Zpracování informací v cloudu

- **NATO Secret on Commercial Hyperscale Briefing:** NATO zvažuje / realizuje konkrétní kroky ke zpracování informací NATO Restricted až NATO Secret v cloudovém prostředí (byla představena roadmapa a nezbytné předpoklady). Nejdříve je cílem zpracovávat informace NATO Restricted, nicméně souběžně budou probíhat práce pro přípravu budoucího zpracovávání až NATO Secret.

The International Counter Ransomware initiative (CRI) – v češtině Mezinárodní iniciativa proti ransomware (CRI)

- CRI je největší mezinárodní partnerská spolupráce v oblasti kybernetické bezpečnosti zaměřená na boj proti kybernetické kriminalitě na státní úrovni, zejména proti ransomware.
- Na konci roku 2024 bylo v rámci této iniciativy zapojeno **68 partnerů**, včetně ČR.
- V rámci CRI díky spolupráci Israel National Cyber Directorate (INCD) a The Cyber Security Council (CSC – UAE) vznikla platforma **Crystal Ball Platform.**
- Jedná se o novou multilaterální platformu pro sdílení hrozeb v rámci zapojených partnerů, podporovanou technologií Microsoft.
- Cíle platformy:
  - Atribuce incidentů a útoků díky sdílení informací o hrozbách v mezinárodním měřítku.
  - Odstrašení kyberzločinců od budoucích útoků díky spolupráci států v reálném čase.
  - Kultivace kultury sdílení informací za účelem více sjednoceného světa.
- Platforma byla navržena v souladu s principem Secure by Design, respektuje také specifické požadavky na umístění dat zapojených partnerů, využívá AI a automatizaci pro zlepšení uživatelského zážitku.
- ČR je v současnosti ve fázi onboardingu (tedy zapojování do aktivního používání platformy).

Jak dále?

- Spolupráce v oblasti kybernetické bezpečnosti je potřeba držet **na velmi vysoké úrovni** zejména ve spolupráci s vládou, akademickým sektorem a soukromým sektorem, včetně nastavení globálním partnerstvím.
- **Budoucnost je v cloudovém prostředí** (hybridní řešení), čistě on-premise řešení jsou v současnosti již přežitkem. Bude nezbytné s dostatečným předstihem a při posouzení všech souvisejících rizik se na tuto skutečnost připravit. Nejít však extrémní cestou, jakou byla donucena Ukrajina.
- **Budoucnost je také ve využití AI nástrojů** (tam, kde to má smysl) a je pravděpodobné, že se AI nástroje rozšíří do velké části běžného života. Ale! Stejně jako jakékoliv jiné nástroje, je potřeba i nástroje AI využívat bezpečně (veřejné / neveřejné modely, školení uživatelů a administrátorů, . . .).

- **Optimistický scénář:** AI řeší klimatické krize, nemoci, chudobu, lidé žijí v éře bez práce s univerzálním příjmem.
- **Pesimistický scénář:** AI způsobí kolaps společnosti (události typu „Terminátor“ nebo „Matrix“).
- **Smíšený scénář:** AI kombinuje přínosy i rizika, AI se stane mocným nástrojem, ale lidská kontrola a etika zůstanou klíčové, úspěch bude závislý na rovnováze mezi technologickým pokrokem a odpovědným řízením.

- Turbulentní vývoj ve směr růstu a rozvoje AI (soupeření USA, EU, ČLR).
- Využití AI v oblasti vzdělávání a práce (personalizované učení, automatizace profesí jako administrativa, call centra).
- Specializovaná AI (výzkum, farmacie, lékařství).
- Běžné využití AI v menších firmách i jednotlivci.
- AI bez nutnosti připojení na internet.
- Zdokonalený malware a škodlivý kód obecně.
- Zdokonalený phishing a deepfake.

Co je pravé?

Děkuji za pozornost.