# Vzdělávací modul
# Kybernetická bezpečnost

Vzdělávací kurz pro vedoucí pracovníky a management, zejména ředitele, finanční ředitele a další decision makery

**Tento modul je financován jako projekt v rámci 5. výzvy z prostředků ESF a státního rozpočtu ČR pod registračním číslem CZ.1.07/3.2.04/05.0014.**

**Tým NSMC**
info@nsmcluster.com

# OBSAH

KYBERNETICKÁ BEZPEČNOST

- Slovo úvodem
- Představení
- Pojmosloví
- CSIRT

# ÚVOD

KYBERNETICKÁ BEZPEČNOST

náš reálný svět je dnes již na fungování toho digitálního **kriticky závislý**

| | | |
|---|---|---|
| banky, | průmyslové podniky, | nemocnice, doprava, |
| výroba, | energetika, | správa přírodních zdrojů, |
| předpověď počasí, | vzdělávání i zábava, | veřejná správa |

… vše je dnes závislé

*Zdroj: vlastní zpracování NSMC*

# ÚVOD

KYBERNETICKÁ BEZPEČNOST

- **pojmosloví**

pokud “jeden mluví o koze a druhý o voze”, pak nedosáhnou výsledku, i když používají stejná slova.

- Počítačová bezpečnost,
- počítačová kriminalita,
- neexistence hranic,
- neurčitost útočníka a
- ochrana národního kybernetického prostoru

# POJMOSLOVÍ

KYBERNETICKÁ BEZPEČNOST

## BEZPEČNOST

- Slovníkové opisy pojmu
- Český slovník pojmů kybernetické bezpečnosti
- Vymezení pro potřeby výuky

# POJMOSLOVÍ

KYBERNETICKÁ BEZPEČNOST

## KYBERPROSTOR - NEEXISTENCE HRANIC

- Prostor je spojité prostředí rozkládající se bez hranic všemi směry, to je první podmínka pro konstatování jeho existence
- Kyberprostor nemá vzdálenosti, jak je chápeme v rámci reálného světa
- Kyberprostor nemá ani žádný rozměr
- Nelze tedy spoléhat na to, že se někde u Starého Hrozenkova, u Aše nebo jinde “na čáře” data zastaví k proclení nebo přeshraniční kontrole

# POJMOSLOVÍ

KYBERNETICKÁ BEZPEČNOST

## KYBERPROSTOR - NEEXISTENCE HRANIC

- Vnitřní velikost kyberprostoru je velmi velká, až blížící se **nekonečnu**.
- Vždy lze připojit další úložiště, nebo uživatele.
- Je-li limitován, pak jen dočasně technickou stránkou růstu infrastruktury a limity vývoje technologií.
- Je zde možno pozorovat něco, co lze připodobnit k hledání konce duhy. Ať se snažíte jakkoliv, stejně jako nikdy nenajdete konec duhy, nelze najít konec kyberprostoru.

# POJMOSLOVÍ

KYBERNETICKÁ BEZPEČNOST

## KYBERPROSTOR - NEURČITOST ÚTOČNÍKA

- Výhodou různých forem distančních útoků z hlediska útočníka nebo útočníků je možnost ukrýt se za přezdívku, tzv. „**nick**“,
- nebo za jiný neurčitý identifikátor, či dokonce za celou kaskádu anonymizačních nástrojů, postupů a falešných identit včetně
  - multiplikace nebo naopak
  - agregace identit a atributů, které by mohly vést k jejich odhalení.

- Útoky prováděné pod rouškou anonymity jsou agresivnější, zákeřnější a využívají metody, které by útočník při přímém kontaktu, kdy je jeho totožnost zpravidla známa, ve většině případů nepoužil – anonymita mu totiž dodává dojem nepolapitelnosti.

# POJMOSLOVÍ

KYBERNETICKÁ BEZPEČNOST

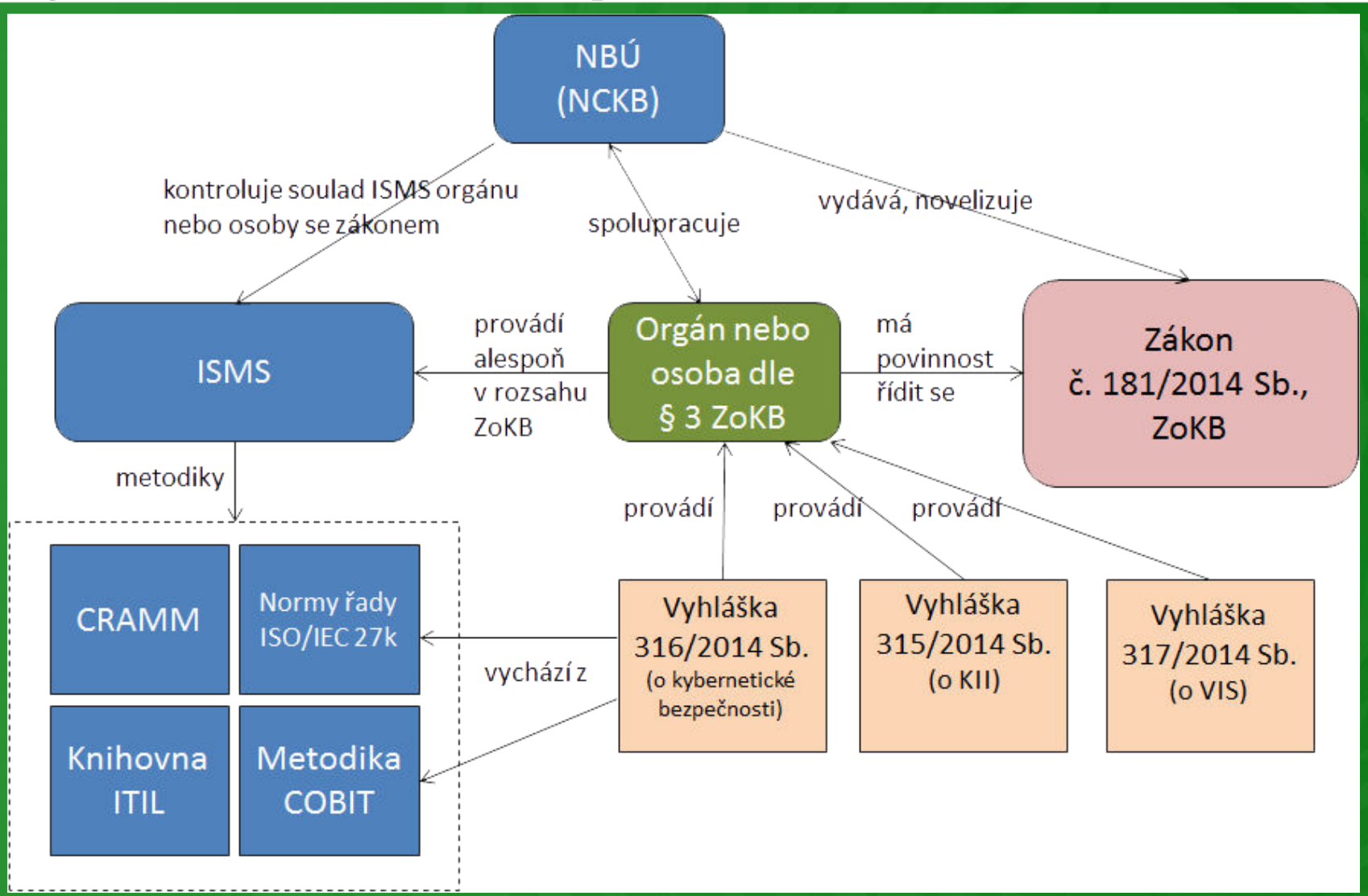
## OCHRANA NÁRODNÍHO KYBERNETICKÉHO PROSTORU

- Pro účinný postup bezpečnostních institucí proti bezpečnostním hrozbám v kyberprostoru je nezbytná široká mezinárodní spolupráce bezpečnostních institucí i s dalšími subjekty, které se zabývají vývojem nových technologií.

- Úlohy
  - sledování aktuálních trendů
  - spolupráce proti cílenému napadání nebo poškozování informačních a komunikačních systémů

# Ochrana národního kybernetického prostoru

KYBERNETICKÁ BEZPEČNOST



# CSIRTy

KYBERNETICKÁ BEZPEČNOST

- CERT (Computer Emergency Response Team)
- CSIRT (Computer Security Incident Response Team)

☑ Základní povinností každého CSIRT týmu je spolupráce při řešení incidentů („response“).

☑ Obvykle CSIRT tým řeší problém, který se vyskytne v rámci jeho pole působnosti (např. vlastní síťové infrastruktury), tedy tam, kde má reálné možnosti k zásahu.

# CSIRTy

KYBERNETICKÁ BEZPEČNOST

na úrovni jednotlivých organizací


ISP, poskytovatelé služeb a obsahu

banky

# NÁRODNÍ A VLÁDNÍ CSIRT TÝMY

KYBERNETICKÁ BEZPEČNOST

- Národní CSIRT
- Vládní CSIRT

- jsou speciální formou CSIRT týmů.
- Jednají s ostatními CSIRTy jako rovný s rovnými, ale jejich role v celém systému je odlišná.

# NÁRODNÍ A VLÁDNÍ CSIRT TÝMY


- Národní CSIRT
  - Last resort – poslední instance, u které je možné žádat o zásah a pomoc
  - cíl: v rámci státu zprostředkovat kontakt mezi napadeným a původcem problému
  - obvykle nevládnou nad fyzickou infrastrukturou
  - věnují se vzdělávání a spolupráci
  - podporují vytváření dalších CSIRT týmů v zemi
  - poskytují podporu při zavádění standardních postupů a procedur

- Vládní CSIRT se zaměřuje na oblast státní správy a samosprávy a na řešení incidentů, které ohrožují bezpečnost státu a jeho služeb.
- Vládní CSIRT může mít podobu týmu interního s možností přímého zásahu v případě problému. Jeho existence je obvykle podpořena legislativně.

# CSIRTy

KYBERNETICKÁ BEZPEČNOST

- ☑ Situace však může být různá
  - ☑ Jsou země, kde funguje pouze národní tým (a plní funkci vládního),
  - ☑ jsou země, kde funguje vládní (a plní roli národního),
  - ☑ jsou země, kde existují oba,
  - ☑ jsou země, kde není ani jeden a roli vrcholového týmu supluje jeden z existujících týmů a pod.

Hierarchie?

- Ve světě CSIRT/CERT týmů je klíčová **ochota sdílet důležité informace o incidentu a hrozbách**. K tomu je nezbytné, aby si týmy navzájem důvěřovaly a také aby svým týmům věřili uživatelé.

# CSIRTy - ENISA

KYBERNETICKÁ BEZPEČNOST

**Agentura pro elektronickou a informační bezpečnost - ENISA**

- Nařízením Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. 3.2004
- sídlí v Řecku ve městě Hérakleion na ostrově Kréta.

- Cílem je zvyšovat schopnost Evropské unie (EU), zemí EU a průmyslu předcházet obtížím v oblasti bezpečnosti sítí a informací, zvládat je a reagovat na ně.
- Kromě toho ENISA poskytuje podporu a poradenství Komisi a zemím EU, např. v technické přípravné práci pro aktualizaci a rozvíjení právních předpisů EU.
- ENISA dále podporuje a prohlubuje spolupráci různých subjektů činných ve veřejném i soukromém sektoru pro dosažení dostatečně vysoké úrovně bezpečnosti v zemích EU.