



# ISMS VE SDRUŽENÍ CESNET

**Andrea Kropáčová**  
CESNET

---

**10. 12. 2020**

**Praha**

- Provozovatel **e-infrastruktury CESNET**
- Založen v roce 1996
- 27 členů (české VŠ, AV ČR) a cca 350 dalších organizací
- K e-infrastruktuře CESNET se mohou připojit instituce, které se zabývají
  - vědou, výzkumem, vývojem včetně uplatnění jejich výsledků v praxi
  - experimentálním vývojem nebo inovacemi v průmyslu i jiných oborech
  - šířením vzdělanosti, kultury a prosperity
  - vybrané sítě veřejné správy
- Hlavní cíle sdružení:
  - výzkum a vývoj informačních a komunikačních technologií
  - budování a rozvoj e-infrastruktury CESNET určené pro výzkum a vzdělávání
  - podpora a šíření vzdělanosti, kultury a poznání

Důvěryhodný  
operátor





- Ochrana e-infrastruktury CESNET a ochrana uživatelů
  - cca 500tis individuálních uživatelů, cca 350 organizací
- Hrozby číhají všude, uživatel je snadným cílem
  - malware, ransomware, cryptolocker
  - podvodné zprávy
- Legislativní důvody
  - zákon o kybernetické bezpečnosti (181/2014 Sb.)
    - CESNET je povinným subjektem
      - písmeno b) paragrafu 3) ... provozovatel významné sítě
      - písmeno h) paragrafu 3) ... poskytovatel digitálních služeb
  - nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), nebo „GDPR“

- Zajištění bezpečnosti poskytovaných služeb (dostupnost, důvěrnost a integrita dat v informačních a komunikačních systémech sdružení),
- zajištění kontinuity provozu poskytovaných služeb,
- ochrana aktiv Sdružení,
- efektivní řízení (bezpečnostních) incidentů a jejich předcházení,
- rozvoj znalostí v oblasti řízení bezpečnosti tak, aby mohly být sdíleny s členy Sdružení;

To vše v souladu se zákony a regulatorními požadavky České republiky a Evropské unie...

- Systém řízení bezpečnosti informací
  - soubor pravidel zajišťující bezpečnost informací
    - tedy dostupnost, důvěrnost a integritu informací
- Východiska
  - ČSN EN ISO/IEC 27001:2014
  - Zákon o kybernetické bezpečnosti



- ISMS scope v CESNET – všechny činnosti, služby a procesy
- Červen 2018: certifikační audit
- Červen 2019: 1. dozorový audit
- Červen 2020: 2. dozorový audit
- Červen 2021: recertifikace



- Splnění zákonných povinností (ZKB, VKB)
- Label kvality
- „Debordelizace“
- Databáze aktiv
  - popis
  - ohodnocení
  - garant

**==> globální inventory „co máme“, „co provozujeme“ ...**
- Analýza rizik
  - čas na zamyšlení ...
  - identifikace a náprava
  - snižování rizik

**==> proces, který bezpečnosti dává „formu“**

- Zavedení pravidel (i nepopulárních)
  - klasifikace informací (především v oblasti práce s dokumenty)
  - bezpečnost je akcentována ve všech aspektech fungování organizace
    - provoz
    - práce s informacemi
    - vývoj
    - zadávací řízení
- Příležitost odhalit a začít řešit dlouho neřešené problémy
  - zaměstnanci nevěděli jak
  - nemělo to prioritu, nebyla vůle
  - bylo to podceňované

**==> schéma ISMS pomáhá s určením závažnosti a urgentnosti, odbourává subjektivní náhled**



- Zapojení zaměstnanců
    - mají prostor se vyjádřit
    - mají možnost něco ovlivnit
  - Zapojení managementu
    - vyjasnění kompetencí
    - jasná specifikace a kvantifikace požadavků
      - technika, know-how ...
      - lidské zdroje
- ==> „bezpečnost něco stojí“**
- Bezpečnost má „životní rytmus“ ;-)
    - PDCA cyklus
    - školení, období horečné aktivity, získání certifikátu, analýza rizik, návrh řešení identifikovaných problémů ...



- Každý uživatel je součástí procesu bezpečnosti
- Cílem není stav „nemáme žádná rizika“
- O rizicích je především potřeba vědět a vědět jak se dají snížit/eliminovat.

Děkuji za pozornost.

Andrea Kropáčová, [andrea@cesnet.cz](mailto:andrea@cesnet.cz)