cesnet

DB AKTIV

TLP: AMBER

Andrea Kropáčová, Marcela Pospíšilová, Jiří Bořík
CESNET

27. 5. 2026
Praha

Upozornění

- ... doplněné do této prezentace na základě dotazů, které jsme obdrželi
- Cílem našich prezentací je sdílet základní informace o řízení bezpečnosti ve sdružení CESNET a poskytnout inspiraci “jak na to”. Nelze je tedy brát jako jediné **správné** či **kompletní** návody a postupy.
- Přehledy aktiv, rizik opatření apod., které jsou uvedeny v našich prezentací jsou pouze příklady a vzorky. Nelze je vnímat jako pro danou oblast kompletní a dostačující výsledky, opět se jedná o inspiraci „jak na to“.

Aktiva, assets ...

Aktiva

- Informační systémy a služby
- HW, SW, aplikace
- Technologie, prostory (sídla organizace, laboratoře, režimová pracoviště)
- Data, informace, know-how
- Zaměstnanci, zákazníci, dodavatelé
- VaV, projekty, vzdělávání
- Vedl. hosp. činnost
- Procesy

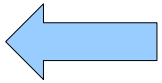
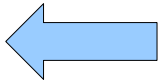
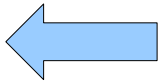
Aktiva

- Informační systémy a služby
- HW, SW, aplikace
- Technologie, prostory (sídla organizace, laboratoře, režimová pracoviště)
- Data, informace, know-how
- Zaměstnanci, zákazníci, dodavatelé
- VaV, projekty, vzdělávání
- Vedl. hosp. činnost
- Procesy
  - typicky „životní cykly“ – např. uživatelské identity, informace (dokumentu), projektu, dodavatele
- Cloudové služby
- API, databáze, SaaS
- Identity a účty
- IoT zařízení

Navazující procesy

- Discovery aktiv
- Klasifikace aktiv
- Ownership aktiv
- Risk management
- Vulnerability management
- Patch management
- Change management
- Incident response
- Business Continuity/disaster recovery
- IAM a identity governance
- Dodavatelský řetězec

Navazující procesy

- **Discovery aktiv** 
- **Klasifikace aktiv** 
- **Ownership aktiv** 
- **Risk management** – téma pro další seminář 18. 6. 2026
- **Vulnerability management**
- **Patch management**
- **Change management**
- **Incident response**
- **Business Continuity/disaster recovery**
- **IAM a identity governance**
- **Dodavatelský řetězec**

Navazující procesy

- **Klasifikace aktiv**
- Každé aktivum musí mít
  - garanta (ownera)
  - technického správce (pověřeného správce)
  - hodnotu, požadavky na DDI
- Je to důležité pro
  - správu
  - řízení změn, kontinuitu činností
  - řízení dodavatelů
  - incident response
  - audit
- Častý nešvar
  - „toto spravuje oddělení XY“
  - NE: Opovědnost musí být jasná a daná!
    - garant = vedoucí daného oddělení/úseku

Navazující procesy

- **Discovery aktiv (objevování a ověřování aktiv)**
- Jak na to (procesně)
  - rozhovor s garantem – analýza na základě znalosti
  - síťové skenování
  - cloud discovery
  - inventarizace endpointů
  - SaaS discovery
  - shadow IT discovery
  - mapování závislostí
- Nástroje
  - Microsoft Defender
  - Lansweeper
  - Tenable (Nessus)
  - Qualys
  - CMDB systémy
- Nálezy
  - neznámé endpointy, staré a zapomenuté zařízení
  - neřízené SaaS, cloudy ...

Nejčastější problémy

- ... při správě DB aktiv

- Kupodivu **NE** technologie
- Ale udržování aktuálnosti **ANO**

- Proč?
  - *obecně těžkopádnost organizací*
  - cloudy (vznikají a zanikají rychle)
  - DevOps vše mění
  - shadow IT roste
  - SaaS proliferace

- Řešení?
  - pravidelná aktualizace, min 1x ročně
  - vhodné technické nástroje
  - úzká spolupráce s garanty a správci

Aktualizace DB aktiv - checklist

- Máme nové aktivum?
- Rozpadáme aktivum na větší detail?
- Rušíme aktivum?
- Popisné informace – garant, správce, DDI, hodnota, HW, SW, fyzické umístění
- Závislosti
  - na jiných aktivech organizace
  - na službě třetí strany
- Související procesy
- Dokumentace
- Dissaster Recovery
- Testy business kontinuity
- Dodavatelé
  - plní VD smluvní ujednání?
- Změny
  - jaké proběhly?
  - jaké jsou v plánu? --> významná změna

Dotazy na garanta a správce

- Záznam o aktivu
  - garant, správce, hodnota, DDI
  - co to je, k čemu to je
  - z čeho se to skládá – HW, SW, aplikace
  - správa – patch management, zálohování, logování
  - s jakými informacemi to pracuje
  - kdo tam má přístup
  - dodavatelé
  - ...

Dotazy na garanta a správce

- Záznam o aktivu
  - garant, správce, hodnota, DDI
  - co to je, k čemu to je
  - z čeho se to skládá – HW, SW, aplikace
  - správa – patch management, zálohování, logování
  - s jakými informacemi to pracuje
  - kdo tam má přístup
  - dodavatelé
  - ...
  - na čem je závislé?
  - je to závislé na nějaké službě třetí strany?
  - co používáte v souvislosti se správou tohoto aktiva?

Dotazy na garanta a správce

- Záznam o aktivu
  - garant, správce, hodnota, DDI
  - co to je, k čemu to je
  - z čeho se to skládá – HW, SW, aplikace
  - správa – patch management, zálohování, logování
  - s jakými informacemi to pracuje
  - kdo tam má přístup
  - dodavatelé
  - ...
  - na čem je závislé?
    - *... na síti, AAI, doméně*
    - *... mám na GoogleDrive instalační soubor, bez kterého to nenajede*
  - je to závislé na nějaké službě třetí strany?
    - *... DB používáme od organizace ABC*
  - co používáte v souvislosti se správou tohoto aktiva?
    - *... v Githubu máme dokumentaci a postupy a zdrojáky...*

Dotazy na garanta a správce

- Záznam o aktivu (informace, data)
  - garant, správce, hodnota, DDI
  - co to je, k čemu to je
  - jakou nabývá podobu?
    - listinnou
    - digitální
  - kde jsou uložené?
    - listinné – kancelář?, sídlo?, externí archiv?
    - digitální
      - v jakém IS?
      - u nějaké třetí strany? (Github, Confluence, Google...)
  - kdo k nim má přístup (a proč?)
    - zaměstnanci, správci (organizace) ... samozřejmě
    - projektoví partneři?
    - dodavatelé?

Kontrola NÚKIB

- Co bude při kontrole NÚKIB zajímat nejvíce:
  - jak identifikujete aktiva,
  - jak určujete kritičnost,
  - kdo je owner (garant),
  - jak udržujete aktuálnost,
  - jak mapujete závislosti,
  - jak navazují bezpečnostní opatření.

  - ... tedy nejen existence seznamu/DB aktiv

    Ale:

  - ... jestli podle něj skutečně řídíte bezpečnost

Kontrola NÚKIB

- Co bude při kontrole NÚKIB zajímat nejvíce:
  - jak identifikujete aktiva, **reg. služba, seznam činností a služeb, org. s, majetek ...**
  - jak určujete kritičnost, **metodika, rozhovor s garantem, na základě závislostí**
  - kdo je owner (garant), **vedoucí oddělení/úseku**
  - jak udržujete aktuálnost, **1x ročně se sejdeme s garantem a jdeme podle checklistu**
  - jak mapujete závislosti, **analýzou s garanty, technologicky**
  - jak navazují bezpečnostní opatření. **vnitřní předpisy, školení, interní kontroly, testy BCP**

  - ... nejde tedy jen o existenci DB aktiv

    Ale:

  - ... jestli podle něj skutečně řídíte bezpečnost

Co dále ...

- **18. června 2026**, 09:30 – 12:00
  - Analýza rizik
    - obecná
    - varování (ala „Huawei“)
    - pro zadávací řízení

- *červenec – srpen – opakování některého z téma*
  - *jak se neutopit v detailu*
  - *GAP analýza*
  - *jak pracovat s vedením*
  - *jen implantovat nZKB do organizace*

- **FIXME. září 2026**, 9:30 – 12:00 **(termín bude včas oznámen)**
  - Řízení dodavatelů
  - Zpracování varování (od NÚKIB)

Další témata pro tyto semináře

- Logování, aneb § 22 **Zaznamenávání událostí**
- Řízení kontinuity činností
- Provozní dokumentace
- Nástroje pro správu DB aktiv
- Zpracování KBU a KBI, hlášení KBI
- Dopadová analýza, BIA

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz