MUNI

CSNOG 2026

Metodická podpora logování v organizaci

Projekt fondu rozvoje CESNET 2024/2025

Stanislav Špaček

Systematizace logovací infrastruktury

CSNOG 2026

- Co je to?
  - Protipól živelnému přístupu – plánování, dokumentace, procesy
  - Určení rozsahu logování
  - Stanovení rolí stakeholderů
- Pozor na vliv aktuální legislativy na logování
  - Logování je v ČR regulované
  - Jsme v souladu?
  - NÚKIB může provádět audity a udělovat sankce

MUNI

Prostředky systematizace

CSNOG 2026

- Metodiky
  - Soubory procesů, doporučení, a best practises pro provoz infrastruktury
- Procesy
  - Vývojový diagram + popis
- Podpůrné materiály
  - Konfigurace běžných logovacích agentů
  - Automatizace nasazení agentů (Ansible)

MUNI

Tematické oblasti pro metodiky

CSNOG 2026

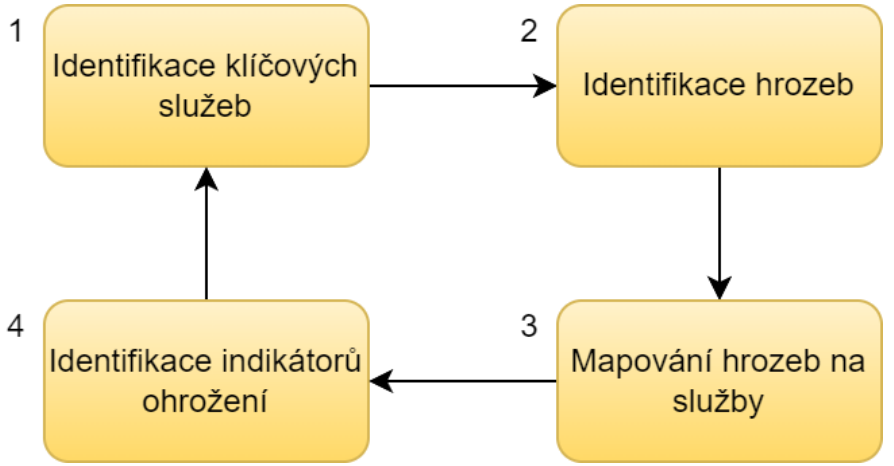
- Zaměření logovací infrastruktury
  - Určení rozsahu logování
  - Odhad nákladů na logování
- Vytvoření a údržba logovací infrastruktury
  - Optimální nastavení logovací infrastruktury
  - Procesy pro běžné operace
- Zpracování záznamu událostí
  - Analýza dopadu zákonů platných v ČR na provoz logovací infrastruktury

MUNI

Zaměření logovací infrastruktury

CSNOG 2026

- Jaké služby a jaké parametry optimálně logovat
- Příklad
  - Klíčová služba: Weby
  - Hrozba: DoS
  - Indikátor ohrožení: počet otevřených spojení na klienta za čas



MUNI

Vytvoření a údržba infrastruktury

CSNOG 2026

- Best practices pro provoz infrastruktury
  - Interpretace času
  - Šifrovaný přenos událostí po síti
- Procesy
  - Přidání logování nové služby
  - Komunikaci se stakeholdery
  - Monitorování infrastruktury
- Dokumentace
  - Knowledge base
  - Uživatelská příručka
  - FAQ

MUNI

Zpracování záznamu informací

CSNOG 2026

- Jak dopadá na logování
  - (Nový) Zákon o kybernetické bezpečnosti, 264/2025 Sb.
  - Zákon o elektronických komunikacích, 127/2005 Sb.
  - Nařízení o ochraně osobních údajů, GDPR 2016/679
- Vymezená témata
  - Jaké události a parametry mají být povinně logovány (NZKB, ZEK)
  - Retence událostí (NZKB, ZEK, GDPR)
  - Řízení přístupů (GDPR)
- Konzultace konkrétních případů s právníky instituce je žádoucí

MUNI

Case study systematizace na MUNI

CSNOG 2026

- Infrastruktura
  - Agenti (syslog-ng, rsyslog, *beat...) -> vector.dev -> OpenSearch, S3
- Vývoj infrastruktury a řízení požadavků
  - Gitlab + issues
- Dokumentace
  - Webové stránky interní a uživatelské
- Procesy definované až na úroveň změn konfigurace (šablony)
- Přínosy:
  - Zalogování nové služby zkráceno z dnů na hodiny
  - Zapojení stakeholderů do vývoje infrastruktury
  - Odhaleno a vyřešeno několik konfliktů s legislativou

MUNI

Summary

CSNOG 2026

- Systematizujte logovací infrastruktury
  - Zrychlení provádění operací a nižší chybovost
  - Efektivnější komunikace mezi stakeholdery
  - Spolehlivější reakce na změny služeb a hrozeb
  - Možná kontrola souladu s legislativou
- Popsané metodiky logování jsou veřejně dostupné jako výstupy projektu Fondu Rozvoje CESNET
  - https://is.muni.cz/publication/2509726/

MUNI

MUNI

CSNOG 2026

Děkuji za pozornost

RNDr. Stanislav Špaček, Ph.D.

spaceks@ics.muni.cz