Perun

Identity and Access Management System

Slávek Licehammer

CESNET

Seminář Univerzitní identity 2016
13. 10. 2016

UNIVERSITAS MASARYKIANA BRUNENSIS

Perun

- IAM - Identity and access management system
- Vyvíjen společně MU a CESNETem
- Kompletní řešení
  - správa identit, skupin, registrací
  - správa služeb a přístupů
  - správa atributů
- Navržen pro integraci do existujících prostředí
- Open source
  - https://github.com/CESNET/perun

Provisioning&deprovisioning

- Propagace identit na služby před prvním použitím
- Zneplatnění účtů
  - Služby s perzistetními daty
  - Služby které jsou aktivní bez uživatelského zásahu (mailing listy, spouštění úloh)
- Plná vs. rozdílová propagace
  - Problém zásahu na straně služby
- SCIM - nekompletní standard

Koncept řízení přístupu

- Technický správce služby
  - Stará se o provoz služby (např. aktualizace)
  - Definuje podmínky použití
  - Jmenuje administrativního správce služby
- Administrativní správce
  - Rozhoduje, kdo smí využívat službu
    - Deleguje toto právo
  - Provádí upřesňující nastavení (např. kvóty)

BANování

- Dočasné zakázání přístupu na službu
- Provádí administrativní správce
- Automatická expirace BANu
- Evidujeme důvod BANu
- Každá služba může na BAN reagovat individuálně
  - Úplné zakázání přístupu
  - Omezení práv

Bezpečnostní týmy

- Zavedení role bezpečnostního týmu
  - Spravuje blacklist uživatelů
  - Stačí zadat identifikátor uživatele (login, EPPN, DN certifikátu)
- Technický správce vybírá kterým týmům důvěřuje
- Uživatelé na blacklistu jsou automaticky blokováni
  - Způsob je závislý na službě
- Technický správce si může založit bezpečnostní tým pouze pro svou službu -> lokální blacklist

Skupinová aritmetika

- Skupina může být členem jiné skupiny (inkluze)
- Přímé / nepřímé členství ve skupině
- Využití
  - Pokročilá workflow
  - Rozdělení pravomocí
  - Spravování výjimek
  - Vizualizace

Děkuji za pozornost

http://perun.cesnet.cz
perun@cesnet.cz

Slávek Licehammer
slavek@ics.muni.cz

CESNET

UNIVERSITAS MASARYKIANA BRUNENSIS