Deprovisioning

Slávek Licehammer
slavek@ics.muni.cz
CESNET

Seminář o bezpečnosti sítí a služeb

cesnet

Motivace

- Služby typicky požadují
  - Autentizaci
  - Autorizaci
  - Atributy uživatelů
- Přesun od lokální správy uživatelů k centralizovaným řešením
  - IdM / IAM systémy, federace identit
- Autorizace je založena na externích informacích

cesnet

Provisioning

- Doručení informací o uživateli službě
  - ACL
  - Autorizační informace (skupiny, role)
  - Atributy uživatele (jméno, email)
- Typicky jsou předávány při přihlášení uživatele
- Někdy jsou tato data ukládána na službě a pouze aktualizována při dalším přihlášení

Implementace provisioningu

- Just in time
  - SAML2, X.509
- Just in case
  - Pull model
    - LDAP, SAML attribute authority, VOOT, SCIM, XML, …
  - Push model
    - Vyžaduje podporu na straně služby

cesnet

Deprovisioning

- Inverzní proces k provisioningu
- Notifikace služby, když uživatel již není oprávněn ji využívat
- Nezbytné pro služby držící data nebo fungující i bez interakce uživatele
  - Mailing listy, datová úložiště, cloudové platformy, výpočetní gridy, ...

Implementace deprovisioningu

- Služba je notifikována bez explicitní akce uživatele (např. přihlášení)
- Reakce na notifikaci je plně v rukách služby
- Způsob deprovisioningu
  - Pull, push
- Protokol závisí na službě
- Nutná podpora na straně služby

Provisioning & deprovisioning

- Provisioning a deprovisioning bývají nasazené společně
- Zajišťují aktuální informace o uživateli na službách
- Zdrojem dat je typicky IdM/IAM
  - Služba nemá online závislost na IdM/IAM

(De)provisioning a reakce na bezpečnostní incidenty

- (De)provisioning lze použít jako nástroj pro mitigaci bezpečnostních incidentů
  - Pozastavení účtu uživatele na službách
  - Nutná implementace vyhodnocení tohoto stavu na straně služby

Požadavky pro implementaci (de)provisioningu

- Nutné minimum
  - Podpora životního cyklu uživatele
  - Správa skupin / atributů / rolí
- Další požadavky
  - Řízení přístupu uživatelů na služby
  - Detekce změn v IdM/IAM a reakce na ně
  - Evidence služeb

Možné řešení pomocí systému Perun

- IdM často nepodporují deprovisioning
- Řešení - externí systém napojený na primární zdroje identit, atributů a skupin
- Perun (https://perun-aai.org)
  - Periodická synchronizace dat z primárních systémů
  - Detekce změn
  - Propagace identit a ACL na služby (push)

Další rozvoj

- Standardizace
  - SCIM?
- Distribuovaná správa uživatelů
  - Služba podporuje více uživatelských komunit, kde každá má vlastní IdM/IAM
  - Částečně se řeší v rámci projektů AARC2 a EOSC-hub


cesnet
DĚKUJI ZA POZORNOST
DOTAZY?