cesnet

NASAZENÍ MFA NA SHIBBOLETH IDP

Jan Oppolzer
CESNET

9. listopadu 2022
Praha

Vícefaktorové ověření:

1. Něco, co víte (jméno a heslo).
2. Něco, co máte (mobilní telefon).
3. Něco, co jste (otisk prstu nebo sken obličeje).

SHIBBOLETH IDP + MFA

- Velmi flexibilní, přihlašovací tok je možné programově upravovat.
- Toky: heslo, X509, IP, Duo, SAML, TOTP, nebo vlastní.
- Toky je možné různě řetězit.
- Uživatelsky i správcovsky nejpříjemnější je Duo, ale není zdarma.
- Námi zvolené řešení využívá TOTP aplikaci v mobilu a webovou aplikaci pro nastavení tokenu do adresářového serveru.

SHIBBOLETH IDP + MFA / TOTP

- Autentizační tok musí být MFA.
  - Začíná tok Password, pak se kontroluje potřeba druhého faktoru.
  - Není-li druhý faktor nutný, je hotovo.
  - Je-li druhý faktor nutný, spustí se to TOTP.

SHIBBOLETH IDP + MFA / TOTP

- MFA na Shibboleth IdP s podporou TOTP:
  - 1. faktor: jméno a heslo,
  - 2. faktor: mobilní telefon,
  - 3. faktor: otisk prstu nebo sken obličeje,
  - 4. faktor: TOTP kód.

cesnet

TOTP

- Shibboleth řeší pouze ověření TOTP, nikoliv nastavení.
- V adresářovém serveru musí být TOTP token jako další atribut.
- Řešení nasazuje profil REFEDS MFA.

cesnet

UKÁZKA

DOKUMENTACE A APLIKACE

- https://www.eduid.cz/cs/tech/idp/shibboleth/mfa
- https://mfa.eduid.cz/

- Webová aplikace 2FA bude k dispozici:
  - Ansible — pro nastavení serveru.
    - Potřeba dodat TLS certifikát.
  - Envoy — pro deployment aplikace.
    - Potřeba dodat konfigurační soubor.

- Dotazy směrujte na info@eduid.cz.

cesnet

DĚKUJI ZA POZORNOST