Alanata
Technology Meets Business

Reálne nasadenie BeyondTrust a praktické skúsenosti z implementácie

Andrej Vávra, Alanata

ANOTÁCIA

Alanata

Budeme prezentovať praktické skúsenosti z nasadzovania produktu BeyondTrust Password Safe, ktorý zabezpečuje správu privilegovaných používateľov a ich prístupov.

Spomenieme motiváciu nasadzovať tento produkt, napr. kvôli legislatívnym požiadavkám. Zameriame sa aj na problémy, ktoré vznikajú a môžu ohroziť úspešnosť celého projektu.

MOTIVÁCIA PRE NASADENIE

Alanata

Čo rieši BeyondTrust Password Safe (PS) ako PAM (Privileged Access Management) riešenie?

- Riadenie prístupu koncových používateľov k privilegovaným systémom a účtom
- Monitoring / audit činností koncových používateľov

Základný use case pre koncového používateľa PS:

- Bezpečné pripojenie sa do internej siete (VPN alebo Privileged Remote Access)
- Koncový používateľ sa autentifikuje do PS pomocou MFA (multi factor authentication). Kliknutím sa pripojí na cieľový systém bez nutnosti zadávať meno/heslo (transparentne). Spojenie na cieľový systém sa realizuje cez PS
- Alternatíva cez Direct Connect. Koncový používateľ sa pripojí na cieľový systém zo svojho connection manager. Rozdiel je ten, že sa autentifikuje voči PS a nie voči cieľovému systému. Na cieľový systém je pripojený transparentne

MOTIVÁCIA PRE NASADENIE

Alanata

Legislatívne požiadavky vyplývajúce zo smernice rámci NIS2

- NIS. Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Je nositeľom základných európskych pravidiel v oblasti kybernetickej bezpečnosti.
- NIS2. Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice 2016/1148, ktorá pôvodnú Smernicu NIS nahradí.
- Členské štáty musia stihnúť pretaviť znenie NIS2 do októbra 2024 do svojich legislatívnych rámcov.
- Dôležitou súčasťou naplnenia NIS2 direktívy bude aj implementácia “Privileged Account and Session Management”riešení.

ROZSAH NASADENIA

Alanata

Odpoveď na otázku: Kto sú používatelia BeyondTrust Password Safe (PS) a aké sú privilegované systémy a účty?

Typy používateľov PS systému: Externisti, Vývojári, Administrátori, ...

Typy koncových systémov a účtov integrovaných do PS z pohľadu:

- Tier (Prod, Test, ...)
- Platformy (Windows, Linux, Network, Web aplikácia, ...)

Možné problémy:

- Príliš veľký scope a cieľe už na začiatku

ROZSAH NASADENIA

Alanata

Upraviť pracovné postupy pre dané typy používateľov a cieľové privilegované systémy a účty

Možné problémy a riešenia:

- Pripojenie na cieľový systém / účet sa realizuje výhradne cez BeyondTrust Password Safe
- Koncový používateľ už nepracuje z „vlastného“ notebooku
- Použitie vlastných nástrojov (connection manager)
- Jump host farma (RDS licencie, zálohované home adresáre)
- File server pre prenos súborov

MFA

Alanata

Prečo je nutná MFA (Multifactor Authentication)?

Ideálne je použiť už nasadené MFA riešenie. Riešime

- akceptáciu od používateľov
- procesy pre enrollment, re-enrollment, ...

BeyondTrust Password Safe má vlastný TOTP server. Možná je integrácia s existujúcim MFA riešením pomocou SAML alebo RADIUS

Pozor na integráciu MFA v connection manager.

AUTOMATIZÁCIA

Alanata

Automatizácia pre procesy:

- Onboarding (nový systém, nový účet, nový používateľ).
- Revokácia prístupu
- Zmena hesiel / SSH kľúčov

BeyondTrust Password Safe (PS) poskytuje možnosti cez:

- Využitie MS Active Directory (používatelia, počítače, skupiny)
- PS Discovery Scan
- PS Smart Rules
- PS technické účty

BREAK GLASS PROCEDÚRA

Alanata

Čo rieši Break Glass procedúra?

PAM systém sa môže stať Single Point of Failure. Ak je PAM nefunkčný, tak sa nikto nikam neprihlási.

Poznámka: PAM sa musí vždy nasadiť v móde vysokej dostupnosti. Napriek tomu môže nastať havarijná situácia.

Čo robiť a ako:

- Obnoviť sieťové (network) spojenia
- Pripojiť sa na cieľové systémy mimo PAM
- Využi Emergency Jump Host, Emergency Passwords

INTEGRÁCIE

Alanata

„Povinné“ integrácie ako každý iný produkt: Email server, MS Active Directory, Monitoring, Backup

Špecifické PAM integrácie:

- MFA riešenie
- Security monitoring
- Ticketovacie systémy

PAM AUDITOR

Alanata

V našich podmienkach nie je možné personálne zabezpečiť nepretržitý dohľad nad PAM.

Predpoklad: Auditor pracuje s PAM iba pri riešení konkrétneho incidentu.

PAM riešenie musí pre audítora zabezpečiť:

- Ukladanie nahrávok sessions a metadát s danou retenciou
- Manuálnu aj automatickú tvorbu reportov podľa daných kritérií
- Automatickú notifikáciu o podozrivých aktivitách