COMGUARD

cyber security masters

WALLIX PAM4ALL

Správa privilegovaných přístupů nejen v zájmu NIS2

Lukáš Babčický

18.09.2023

WALLIX Group

- Francouzská společnost s 20 lety působnosti
- Leader v oblasti PIM / PAM
- Silné zaměření na OT security

KUPPINGERCOLE

Leader 2020-2022

FROST & SULLIVAN

V roce 2022 byl PAM4ALL vyhodnocen jako nejlepší dostupné PAM řešení s ohledy na flexibilitu, jednoduchost a cenu.

2022 Customer Value Leadership Award

Gartner

Velmi rychlý posun na **globálního Leadera** v roce 2022

2022 SPARK MATRIX LEADER

QUADRANT KNOWLEDGE SOLUTIONS

Leader v prvním vydání Spark Matrix PAM

WALLIX Authenticator
MFA

WALLIX Access Management
Správa vzdálených přístupů

WALLIX Session Management
Správa relací

WALLIX BestSafe
Princip nejnižších oprávnění v praxi

WALLIX Password Management
Správa životního cyklu přihlašovacích údajů

SSO proxy

- Prosazení autorizačních politik na druhotná spojení
- Pokročilé přístupové politiky – Časové rámce, podmínky
- Integrace s Password Vaultem

NIS2: § 19 - Bezpečnost komunikačních sítí - P.O. zajistí:

- řízení vzdáleného přístupu ke komunikační síti
- řízení vzdálené správy technických aktiv
- v rámci řízení komunikace, vzdáleného přístupu a vzdálené správy povoluje pouze takovou komunikaci, která je nezbytná pro řádné zajištění regulované služby

SSO proxy

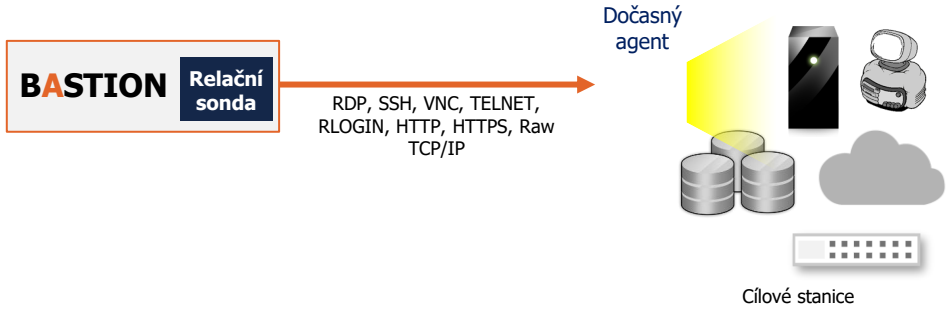
- Prosazení autorizačních politik na druhotná spojení
- Pokročilé přístupové politiky – Časové rámce, podmínky
- Integrace s Password Vaultem

NIS2: § 20 - Správa a ověřování identit / § 21 – Řízení přístupových oprávnění

- Povinná osoba používá nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv regulované služby. Nástroj zajišťuje:
  - ověření identity před zahájením jejich aktivit,
  - opětovné ověření identity po stanovené době nečinnosti,
  - centralizovanou správu identit s ohledem na vazby mezi aktivy.

Monitoring a auditing

- Sledování a sdílení relací
- Auditní záznamy relací
  - Session probe
- Kontrola průchozích souborů via ICAP
  - DLP
  - AV / sandbox



Správa a rotace hesel

- Integrace s Password Vaultem
- Management hesel a SSH klíčů
  - Automatická rotace
  - Definice komplexity a periodicity
  - App-to-App Password Management

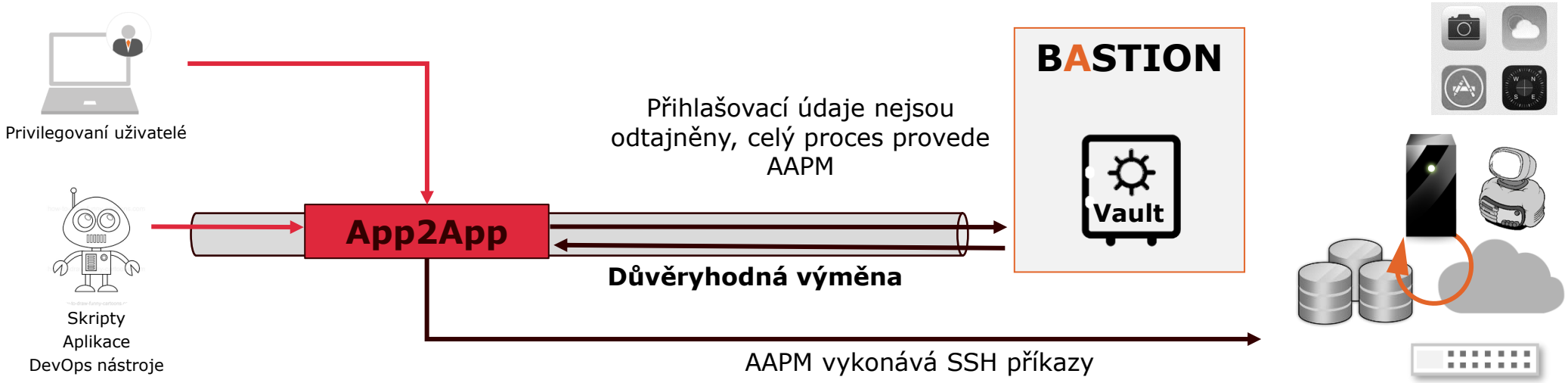
NIS2: § 20 - Správa a ověřování identit

Povinná osoba používá nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv regulované služby. Nástroj zajišťuje:

- odolnost uložených a přenášených autentizačních údajů vůči hrozbám a zranitelnostem, které by mohly narušit jejich důvěrnost nebo integritu,

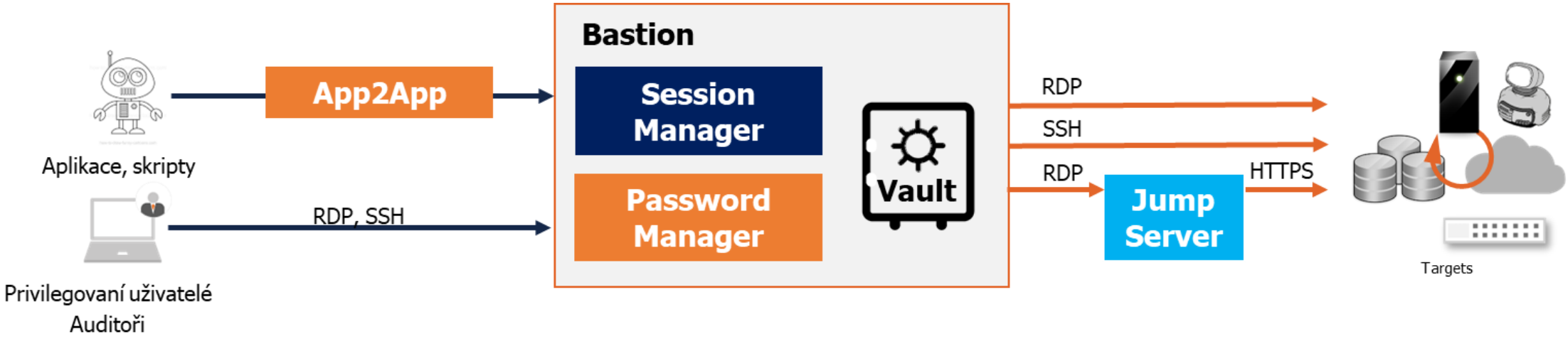
Application to Application Password Management

- Řešení pro zabezpečení přihlašovacích údajů u automatizovaných úkonů:
  - DevOps či skripty
- Efektivní náhrada hardcoded hesel
- AAPM vyzvedne credentials z Vaultu a provede úkon definovaný skriptem



Architektura

- RDP / SSH proxy
- Dostupné jako AIO appliance
  - Debian based, hardened
- HW / Virtual / Cloud



Zajištění přístupu k OT

- Enkapsulace propritetárních protokolů do SSH
- Nemění operátorská workflows

Zajištění přístupu k OT

- Enkapsulace propritetárních protokolů do SSH
- Nemění operátorská workflows

NIS2: § 28 - Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

- omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům
- omezení vzdálených přístupů a vzdálené správy průmyslových, řídicích a obdobných specifických technických aktiv

Privilege Management

- Prosazení principu nejnižších oprávnění
- Standalone agentský nástroj / Komponenta PAM

- Umožní eliminaci administrátorských oprávnění
- Hardening účelových PC

NIS2: § 14 - Řízení přístupu

Povinná osoba dále v rámci řízení přístupu k aktivům:

- omezí přidělování administrátorských a privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce

WALLIX zajistí:

- Kompletní správu privilegií a privilegovaných přístupů
- Flexibilitu nasazení
- Jednoduchou implementaci a provoz

COMGUARD

cyber security masters

Děkujeme za pozornost!