DŮVĚŘUJTE, ALE PROVĚŘUJTE

SPRÁVA A DOHLED PRIVILEGOVANÝCH ÚČTŮ

Privilegované účty umožňují na základě vysokých oprávnění vašim správcům a administrátorům spravovat Vaše servery, systémy, aplikace, software a data. Privilegovaný účet nemusí reprezentovat jen konkrétního uživatele, ale může být non-human a reprezentovat jen službu, aplikaci nebo úlohu.

CO JE TO PAM?

Privileg Access Management (někdy také Privileged Account Management) označují nástroj nebo systém pro:

- Správu a zabezpečení privilegovaných účtů.
- Řízení jejich bezpečného použití k přístupu ke kritickým systémům a datům.
- Dohled nad činnostmi uživatelů, kteří privilegované účty používají.

RIZIKA SPOJENÁ S PRIVILEGOVANÝMI ÚČTY

- Jeden účet nebo jeho heslo se používá pro více systémů.
- Použití jednoduchých nebo defaultních hesel.
- Sdílení přihlašovacích údajů (se třetími stranami, pro zjednodušení správy…).
- Ukládání hesel ve sdílených souborech (Excel, Word…).
- Často mají zbytečně vysoká oprávnění a neexspirují.
- Často zůstávají v infrastruktuře aktivní, a přitom si jich nikdo nevšímá a nepoužívá je.
- Získání privilegovaných údajů je často umožněno získáním přístupu k běžnému účtu.

Tyto účty představují největší možné bezpečnostní riziko. Řešení PAM umožní organizacím lépe kontrolovat tyto účty a sledovat, kdo má přístup k jakým systémům, kdy a na jak dlouho. Nasazuje se na kontrolu a auditování aktivit vykonávaných dodavateli a také interních správců.

NABÍZÍME SYSTÉMY PRO VŠECHNY VAŠE POTŘEBY

PASSWORD MANAGEMENT

- Ukládání hesel v zabezpečeném (šifrovaném) trezoru.
- Lokální nebo sdílená instalace.
- Browser plugins/extensions.
- Auto-fill do webových formulářů.
- Kontrola síly a stáří hesla.
- Generování hesla.

Usnadňuje zaměstnancům použití komplexnějších hesel a jejich obměnu.

PRIVILEGE ACCOUNT MANAGEMENT

- Automatická změna hesel.
- Checkout procedury.
- Schvalovací workflow.
- Role-based přístup.
- Pokročilý audit a reporting.
- Integrace s různými systémy (AD, SIEM).
- HA, automatické zálohy.

Pokročilejší sdílení údajů privilegovaných účtů a jejich správa.

PRIVILEGE ACCESS MANAGEMENT

- Přímý přístup k systémům.
- Integrace s enterprise systémy (IDM, Remote Management, DevOps, API).
- Behaviorální analýza.

Bezpečné používání a správa privilegovaných účtů. Dohled nad přístupem privilegovaných uživatelů k důležitým datům a systémům (cíle).

RADIM PRACUCH | PRACUCH@DATASYS.CZ | +420 724 065 027

Nástroj EKRAN v informačním systému ustavuje proces trvalého průběžného monitorování činnosti administrátorů. Od momentu nasazení poskytuje systém detailní indexovaný „videozáznam“ relací s metadaty. Díky tomu je možné snadno analyzovat i několikahodinové relace. Kontrola činností privilegovaných účtů je tak velmi srozumitelná a naplňuje jedno z nejdůležitějších bezpečnostních opatření ve Vaší firmě.

KLÍČOVÉ VLASTNOSTI

- **Rychlé nasazení** – implementace zabere pouze jednotky hodin a nevyžaduje změny v postupech
- **Nejlepší nástroj** – pro zaznamenání a auditování uživatelských relací
- **Výborná cena** – nízkonákladové řešení
- **Bezkonkurenční licenční politika** – umožňuje přesouvat licence na monitorované servery

Nástroj WALLIX Bastion je nejsnáze nasaditelné centralizované řešení privilegovaných přístupů pro nahrávání a sledování privilegovaných relací. Umožní vám definovat bezpečnostní politiky pro kontrolu přístupů účtů s rozšířeným oprávněním. Obsahuje možnost vynucení pravidel pro jednotlivé uživatele. Skládá se z Password managementu a Session managementu, který je v tomto případě silnější. Volitelným modulem je Access Manager sjednocující přístup a správu více Bastion serverů

KLÍČOVÉ VLASTNOSTI

- **Rychlé nasazení –** implementace zabere pouze jednotky hodin
- **Snadná integrace –** bezproblémově zapadne do současného prostředí
- **Variabilní možnosti nasazení –** HW / Virtual Appliance / AWS / Azure
- **Jednotná správa –** centrální konzole pro definice politik a reporting
- **Proxy architektura –** není třeba instalovat agenty na koncové systémy
- **Vyhledání privilegovaných účtů –** komponenta WALLIX Discovery
- **Zvýšení produktivity externistů –** relace jsou nahrávány a uchovávány
- **ICS/SCADA –** zabezpečení přístupu k průmyslovým kontrolním systémům
- **Správa hesel –** Password Manager zajišťuje komplexitu a obměnu hesel

Bezpečnostní nástroj Thycotic omezuje rizika privilegovaných účtů, implementuje zásady nejmenších privilegií, řídí aplikace a bezpečně ukládá sdílená hesla a SSL klíče. K přístupu k jednotlivým citlivým údajům jsou oprávněni jen vybraní uživatelé. Tento nástroj má nejlépe propracovaný Password management.

KLÍČOVÉ VLASTNOSTI

- **Zabezpečený trezor –** privilegovaná pověření jsou uložena v šifrovaném centralizovaném trezoru
- **Rozkrytí účtů –** možnost detekce všech účtů služeb, aplikací a správců pro úplný přehled o přístupech
- **Správa hesel a klíčů –** možnost zobrazení hesla nebo jeho poskytnutí pro připojení bez zobrazení hesla, kontrola komplexity hesel, rotace hesel, heartbeat
- **Delegování přístupů na koncové systémy –** podle rolí, postup (workflow) pro žádosti a schvalování přístupů
- **Řízení relací –** proxy vstupní brána, monitorování a nahrávání uživatelských relací s možností zásahu
- **Systém šablon –** pro různé typy privilegovaných údajů, možnost editace a tvorby vlastních šablon

Nástroj	EKRAN	WALLIX Bastion	THYCOTIC Secret Server
Forma dodání nástroje	Aplikace pro Windows Server	„Hardened“ (linux) appliance	Aplikace pro Windows Server
Architektura nástroje	Agentský nástroj s možností Jump serveru	Přístupový portál s možností transparentního režimu	Přístupový portál přímým připojením z klientské stanice nebo prostřednictvím SSH proxy
Password management	▪ Rotace hesel (Windows) ▪ Podpora SSH klíčů	▪ Rotace hesla i klíčů (podpora většiny systémů) ▪ Podpora externích úložišť	▪ **Bohatá knihovna pluginů** ▪ **Podpora externích úložišť** ▪ **Heartbeat**
Access management	▪ Windows / Linux servery ▪ web účty ▪ MS SQL	▪ **Podpora přihlášení k většině systémů a spouštění aplikací (vč. tlustých klientů)** ▪ **Variabilita způsobů připojení (nativní klient, AM + HTML5)**	▪ Využití „launcherů“ s možností customizace ▪ SSH proxy
Session management	▪ **Záznamy relací s bohatými možnostmi konfigurace** ▪ Forenzní export, alerty, reporty	▪ Možnost volby záznamu relací ▪ Možnost manuálního nebo automatického zásahu do relace na úrovni příkazů	▪ Možnost volby záznamu relací ▪ Možnost ukončení relace
Podoba nahrávek	**Indexované snímky obrazovek ve formě video logů**	**Indexované video logy s možností uložení ve formátu mp4**	Video logy s časovou osou aktivit (s možností indexování)