ARICOMA

Privileged Access Management

Pomůžeme vám dostat vaše účty pod kontrolu. Získejte přehled o tom, kdo privilegované účty používá a co tito uživatelé dělají, když jsou přihlášeni.

Správa privilegovaného přístupu je zásadní v každé organizaci, protože privilegované účty představují pro organizaci či firmu značné riziko. Pokud útočník napadne standardní uživatelský účet, bude mít přístup pouze k informacím tohoto konkrétního uživatele. Podaří se mu však kompromitovat privilegovaného uživatele, získá tak okamžitě větší přístup a schopnost sabotovat i další systémy.

Útočníci se zaměřují především na privilegované účty, aby mohli místo jedince kompromitovat celé organizace. S PAM řešením můžeme vyřešit vaše slabá místa v zabezpečení, jako například přístup více uživatelů se znalostí stejného hesla pro konkrétní službu. Snížíte tak riziko pramenící z dlouhotrvajících statických hesel, které správci nechtějí měnit.

PAM systém je určen na ukládání a řízení přístupových údajů účtů s vyššími privilegii, a to s ohledem **na nejvyšší možnou ochranu z pohledu bezpečnosti** a zároveň kontroly a monitoringu přístupů k těmto údajům.

Řešení dokáže řídit různé typy privilegovaných účtů – lokální technické i servisní účty, doménové účty, lokální administrační účty nebo personální účty. Dokáže pokrýt takřka všechny funkční požadavky jako:

- řízení přístupů,
- řízení hesel a SSH klíčů,
- náhrada přihlašovacích údajů natvrdo zapsaných v aplikacích,
- řízení privilegií privilegovaných účtů,
- izolace privilegovaných přístupů,
- real-time auditing,
- detekování podezřelého chování.

S privilegovanými účty zacházíme se zvýšenou péčí. Pokud by se například přihlašovací údaje správce nebo servisního účtu dostaly do nesprávných rukou, mohlo by to vést ke kompromitaci systémů a důvěrných dat celé vaší organizace.

Privileged identity management (PIM)

PIM jsou systémy pro monitorování a ochranu privilegovaných uživatelů v IT prostředí organizace. Přebírají správu privilegovaných účtů a přístupy k nim ukládají do zabezpečeného úložiště (trezoru). Tím zajišťují izolaci použití privilegovaných účtů, aby se snížilo riziko jejich odcizení.

S privilegovanými účty musíme zacházet se zvýšenou péčí. Pokud by se například přihlašovací údaje správce nebo servisního účtu dostaly do nesprávných rukou, mohlo by to vést ke kompromitaci systémů a důvěrných dat celé vaší organizace. Proto se vlastnosti PIM/PAM systémů často slučují do jednoho komplexního řešení.

Výhody

Omezení rizik spojených s privilegovanými účty:

- Zabraňuje kompromitaci systémů a citlivých dat útokem na privilegované účty.

Centrální zabezpečené uložiště:

- Umožňuje centrální evidenci hesel a přístupových údajů.
- Zajišťuje kontrolu přístupu k uloženým heslům a klíčům.

Pokročilé management hesel a SSH klíčů:

- Umožňuje nastavení komplexity hesel a klíčů.
- Zabezpečuje automatickou rotaci hesel a klíčů.
- Provádí validaci hesel a klíčů pro zajištění jejich síly a bezpečnosti.

Zabezpečení a monitoring přístupů:

- Izoluje privilegované přístupy a zajišťuje, že jsou přístupy k citlivým údajům řízeny a monitorovány.

Audit a compliance:

- Umožňuje detailní audit využívání účtů včetně záznamu klávesnicových úhozů a video nahrávek.
- Podporuje dodržování předpisů a interních pravidel týkajících se správy účtů.

Detekce podezřelého chování:

- Systém je schopen rozpoznat neobvyklé aktivity a reagovat na potenciální bezpečnostní hrozby.

Řízení různých typů privilegovaných účtů:

- PAM systém dokáže spravovat lokální technické i servisní účty, doménové účty, lokální administrační účty i personální účty.

Zajištění funkčních požadavků:

- Systém pokrývá potřeby organizace v oblasti řízení přístupů, hesel, SSH klíčů, nahrazení pevně zadaných přihlašovacích údajů v aplikacích a další.

Osvědčené postupy správy privilegovaného přístupu