

Cyber-Ark Privileged Identity Management

La soluzione integrata PIM per la gestione delle utenze privilegiate ed amministrative del sistema informativo

La gestione delle utenze privilegiate è un problema recentemente salito ai massimi livelli di attenzione non solo delle direzioni IT e Sicurezza, ma anche del *top C-level*, grazie alle recenti normative, in particolare del Garante della Privacy in Italia e PCI DSS a livello internazionale, come anche SOX, Basilea2, ecc.

Le utenze privilegiate associate a funzioni di gestione ed amministrazione per sistemi hardware quali *server*, *router* o *firewall* e per software sia di base, come sistemi operativi e DBMS, che di piattaforme applicative, quali ERP, CRM, ecc. sono quindi un eterogeneo universo diventato ormai oggetto di verifiche, monitoraggio e controllo.

La crescita esponenziale della presenza di apparati "intelligenti" nelle reti aziendali da una parte, e di pacchetti software dall'altra, tutti dotati di utenze amministrative predefinite, pone significativi problemi di sicurezza alle aziende. La disponibilità di tali password di accesso amministrativo senza le opportune cautele e controlli, può produrre notevoli danni sia in termini operativi che di accesso ad informazioni sensibili, come dimostrano anche i numerosi casi saliti alla ribalta delle cronache nei più svariati ambiti ed in vari paesi del mondo.

Non è un caso quindi che recentemente siano apparse nuove normative (Garante della Privacy su ADS, *Market Abuse*, *Sarbanes-Oxley Act*, PCI DSS) volte fra l'altro a indurre le aziende a definire e realizzare politiche di gestione più accorte degli accessi ad utenze privilegiate come anche della normale utenza.

Tuttavia, mentre la gestione delle password personali degli utenti finali può essere effettuata attraverso l'utilizzo di comuni sistemi di Identity & Access Management, la gestione delle utenze privilegiate e di amministrazione, non personali, molto spesso più numerose, poiché presenti in modo pervasivo in tutti i sistemi, è attualmente lasciata alla operatività quasi esclusivamente manuale o addirittura non realizzata affatto.

E' prassi comune, ad esempio, che le password amministrative vengano clonate o variate in modo uguale per tutti i sistemi in gestione e modificate assai raramente, talvolta rimanendo così come definite dai produttori.

Cyber-Ark Privileged Identity Management è la prima suite integrata per la completa gestione delle password di utenze privilegiate in uso in una azienda. La suite è composta di tre soluzioni orientate alla gestione delle problematiche di monitoraggio e gestione secondo le varie sfaccettature in cui queste si presentano:

Enterprise Password Vault®: l'infrastruttura applicativa che con tecnologia brevettata mantiene le informazioni protette e ne gestisce la variazione secondo policy aziendali configurabili

Application Identity Manager™: la soluzione che consente la gestione degli accessi privilegiati e di amministrazione effettuati da parte non di persone ma di applicazioni aziendali

Privileged Session Manager™: per la registrazione non solo degli accessi ma anche di tutte le attività svolte nelle sessioni amministrative degli utenti privilegiati

Enterprise Password Vault: *l'infrastruttura compliant*

Conservazione

Enterprise Password Vault è in grado di conservare le password in un sistema hardware altamente protetto (il *Vault* o cassaforte digitale), in modalità conforme alle regolamentazioni esistenti, quali quella del Garante della Privacy sugli Amministratori di Sistema (ADS). In tale cassaforte digitale, installata in una macchina isolata e totalmente "*hardenizzata*", sono anche memorizzati i log degli accessi in modalità *read-only* in formato criptato ed inalterabile da utenti non autorizzati.

Accessibilità

- ✓ Le password memorizzate nel *Vault* sono facilmente accessibili attraverso una applicazione web.
- ✓ Il trasferimento delle informazioni verso gli utilizzatori è protetto automaticamente da un canale altamente crittografato.
- ✓ In generale gli utilizzatori (Sistemisti, DBA, Amministratori) non "conoscono" le password, se non nel momento in cui devono effettivamente utilizzarle e per un periodo di tempo predeterminato. Tali utenti si relazionano al sistema attraverso una identificazione personale.

Controllo

- ✓ Ogni accesso viene automaticamente controllato e registrato e sono prodotte informazioni per attività di auditing. E' configurabile l'invio per e-mail delle segnalazioni di accesso, anche in tempo reale, a destinatari autorizzati.
- ✓ E' possibile prevedere casi di controllo incrociato dell'accesso in tempo reale (autorizzazione contestuale da uno o più autorizzatori).
- ✓ Sono pienamente integrabili meccanismi di *Strong Authentication* (PKI) e utilizzo di *token* e *smart-card*.

Policy di variazione automatizzata delle credenziali

- ✓ E' disponibile un componente di gestione delle *policy* di variazione delle credenziali per gli accessi privilegiati in grado di provvedere automaticamente alla generazione ed all'aggiornamento delle password per tutti i più diffusi sistemi hardware e software. Il componente è facilmente estendibile per gestire sistemi non diffusi o *custom*.
- ✓ La generazione automatica e' ampiamente configurabile in conformità alle varie normative sia in termini di complessità delle password che in termini di periodicità di aggiornamento.
- ✓ Il componente può gestire la notifica dell'avvenuto utilizzo/cambio di una password via e-mail e integrando piattaforme SIEM
- ✓ Gestione di "*one time password*" esclusive.

Gestione credenziali di Terze Parti

Il sistema di gestione delle password offerto da **Enterprise Password Vault** di Cyber-Ark permette una maggior sicurezza ed efficacia nelle definizioni delle policy anche nel contesto di realtà aziendali che facciano uso di terze parti per l'assolvimento di task amministrativi. Il personale in outsourcing pur avendo modo di accedere a tutti i livelli di gestione ai sistemi di interesse non avrà più la titolarità della gestione delle password. La possibilità inoltre di permettere a utenze particolari (es. sviluppatori software, integratori, tester, manutentori) di accedere selettivamente ad utenze amministrative, limitatamente ai periodi di interesse per le attività svolte, consente una significativa semplificazione del controllo di tali attività.