WHITE PAPER | MAGGIO 2017

Privileged access management maturity model per la digital transformation e l'automazione su vasta scala

ca technologies

Sommario

Executive Summary

La sfida

Come ci si può aspettare, le aziende che intraprendono un percorso di digital transformation devono affrontare maggiori problemi correlati a rischi e sicurezza. Le iniziative di digital transformation aumentano inevitabilmente il numero dei punti di accesso all'infrastruttura aziendale che sfuggono ai controlli esistenti, sono accessibili a un numero superiore di set di identità diversi e proliferano all'interno di un'infrastruttura distribuita e dinamica.

L'opportunità

Conoscere i propri utenti con privilegi significa conoscere i rischi. Di per sé, gli strumenti di privileged access management devono essere in grado di supportare l'automazione nel processo di autorizzazione e garantire la scalabilità attraverso il supporto di operations dinamiche e infrastrutture effimere, come gli account amministrativi Amazon Web Services (AWS) per le identità umane.

I vantaggi

Per identificare più efficacemente gli attacchi che si basano sul furto di credenziali non basta accumulare più dati, ma occorre incorporare dati più mirati sul comportamento degli utenti con privilegi, per consentire l'identificazione di cambiamenti significativi che possono essere il sintomo di un rischio reale. Questo approccio viene ulteriormente rinforzato attraverso l'integrazione con sistemi di governance degli accessi con privilegi, per consentire l'analisi comportamentale tra utenti con ruoli paragonabili.

Sezione 1

Introduzione

Il software costituisce l'elemento centrale per competere e gestire efficacemente le aziende del XXI secolo. Storicamente, la tecnologia ha sempre giocato un ruolo chiave nella strategia di business. Con la digital transformation, tuttavia, le iniziative di trasformazione e accelerazione del ciclo di delivery del software e dei processi di sviluppo delle applicazioni sono diventate un imperativo, a tutti i livelli del business, che si sovrappone sempre più a un altro problema pressante per il consiglio di amministrazione: la cybersecurity.

La trasformazione implica necessariamente un cambiamento, che a sua volta comporta un rischio. A mano a mano che le aziende proseguono lungo il percorso di digital transformation, il rischio diventa più elevato, a meno che non abbiano implementato un piano per la protezione e la governance degli accessi che vada di pari passo con le iniziative e rispecchi le priorità di molti piani di digital transformation:

- Abilitare l'automazione garantendo visibilità e misurabilità
- Promuovere la velocità di delivery parallelamente alla protezione degli asset aziendali
- Garantire la scalabilità con una soluzione integrata di governance degli accessi e rilevamento delle minacce

Per garantire visibilità e misurabilità ai fini di compliance, sicurezza e governance, assicurando al tempo stesso la flessibilità necessaria per la digital transformation, è necessario un approccio nuovo e maggiormente allineato alla concessione dell'accesso (chi), e ora anche alla modalità (cosa: ovvero applicazioni, servizi, macchine e oggetti): l'accesso con privilegi.

Così come molte aziende stanno attualmente lavorando alla definizione di una mappa pratica dei propri percorsi di digital transformation, i team di sicurezza devono disporre delle capacità di integrazione e degli strumenti appropriati per automatizzare, accelerare e scalare progressivamente la gestione degli accessi e il contenimento dei rischi, in linea con le esigenze di business, senza richiedere nuovi investimenti importanti.

Sezione 2

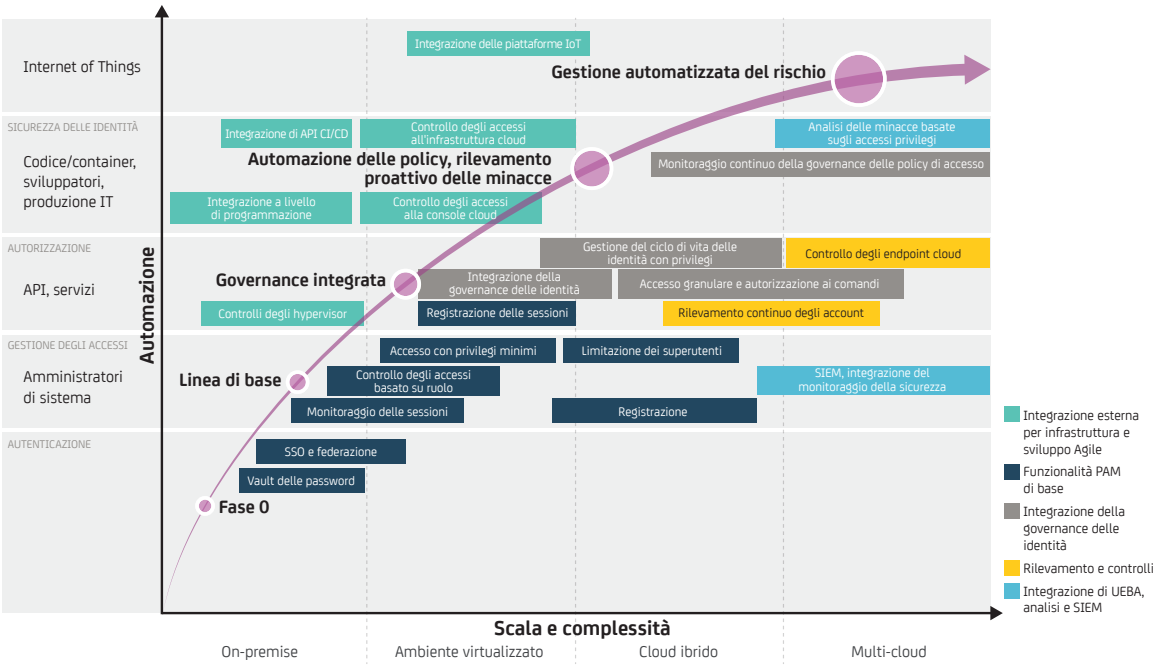
La digital transformation aumenta il rischio associato agli accessi con privilegi

La digital transformation implica necessariamente il cambiamento, l'accelerazione e l'automazione delle modalità di interazione fra codice, macchine e identità umane. I rischi e i problemi di sicurezza si amplificano, perché le iniziative di digital transformation aumentano inevitabilmente il numero dei punti di accesso all'infrastruttura aziendale che sfuggono ai controlli esistenti, sono accessibili a un numero superiore di set di identità diversi e proliferano all'interno di un'infrastruttura distribuita e dinamica (on-premise, virtuale e cloud).

La determinazione delle identità che devono avere accesso a risorse e servizi specifici, la gestione delle relative credenziali per l'accesso alle risorse e la verifica della legittimità di tale accesso con un intervento manuale minimo e basato su policy costituiscono delle sfide cruciali per garantire automazione, scalabilità e velocità.

Inoltre, per stare al passo con la rivoluzione della mobility, oggi le imprese devono prepararsi per la Internet of Things (IoT), che incrementa, con vari ordini di grandezza, il volume delle transazioni all'interno dell'infrastruttura aziendale. In seguito all'adozione degli strumenti per la digital transformation, l'elemento "chi" dell'equazione di gestione degli accessi subisce un cambiamento radicale, ancora prima di introdurre i device IoT nella combinazione.

Affinché il privileged access management possa diventare uno dei principali promotori della digital transformation, anziché un collo di bottiglia, la tecnologia e gli strumenti devono fornire una soluzione consolidata ed estensibile ai rischi introdotti dal percorso di trasformazione.



Governance integrata

Gli approcci manuali che dipendono da un processo di certificazione umano non possono scalare quando la digital transformation aumenta sia il numero degli utenti che hanno bisogno di accesso con privilegi al di fuori dei tradizionali ruoli di amministratore di sistema, sia quello delle entità che possono agire come identità con privilegi. Per bilanciare agilità e sicurezza nei nuovi scenari di accesso (sviluppatori con accesso a credenziali con privilegi in produzione, container e host virtualizzati con autorizzazioni per le origini dati o amministratori con accesso di superutente ai servizi cloud), le richieste di ruoli e autorizzazioni devono essere gestite tramite un processo di governance integrato.

Automazione delle policy

Le architetture ibride di sviluppo e deployment, che includono risorse on-premise, data center virtualizzati e ambienti di cloud pubblico, possono dare luogo a un approccio frammentario e compartimentalizzato alle identità con privilegi. Per garantire la coerenza (ed evitare la dipendenza dal fornitore), è necessario applicare dinamicamente policy centralizzate di controllo degli accessi e governance agli account con privilegi specifici dell'ambiente (come gli account superadmin di AWS).

Rilevamento proattivo delle minacce

Anziché gestire l'accesso a una password condivisa per un'infrastruttura statica, come un server fisico di data center, oggi le imprese devono gestire la modalità di autorizzazione, monitoraggio e registrazione degli accessi alle credenziali con privilegi per un'ora, un giorno o persino alcuni minuti, nonché valutare se le modifiche apportate o le azioni intraprese utilizzando tali credenziali sono legittime e non incrementano il rischio. Adottando un approccio basato sul contesto, che utilizza le funzionalità di machine learning e analisi comportamentale, è possibile promuovere il rilevamento in tempo reale e intraprendere misure di contenimento del rischio, anche negli ambienti più effimeri e dinamici.

Gestione automatizzata del rischio

L'adozione della IoT non si limita a introdurre un nuovo tipo di identità con privilegi per le macchine, sotto forma di controller dei device IoT, ma l'uso della tecnologia contribuisce a un aumento potenzialmente esponenziale del numero delle transazioni che devono essere esplicitamente autorizzate e monitorate per eventuali attacchi. Per gestire le identità e il volume delle transazioni tramite identità con privilegi è necessario un modello automatizzato in grado di rilevare efficacemente le minacce, supportare i meccanismi di valutazione dei rischi e implementare le misure di contenimento, senza interferire in modo significativo con i processi di business.

Sezione 3

Implementare la governance integrata e l'automazione delle policy, passo dopo passo

Gestire e proteggere l'accesso con privilegi nel contesto della digital transformation è un problema pressante, ma non insormontabile.

Ma poiché gli hacker sfruttano sempre più, e con successo, le credenziali degli utenti con privilegi per ottenere accesso non autorizzato, occorre un maturity model per limitare le policy e monitorare i punti ciechi, oltre che per abilitare un modello di rilevamento proattivo attraverso l'analisi basata su machine-learning, che consenta di aumentare il valore degli investimenti attuali e migliorare la precisione.

Per agevolare, anziché impedire, la digital transformation, l'accesso con privilegi a infrastruttura, sistemi sensibili e dati deve essere basato su una serie di fasi realistiche e coordinate nel contesto di un maturity model. La misura più ovvia consiste nel ridurre il numero dei passaggi manuali necessari per il provisioning dell'accesso alle credenziali con privilegi, collegando le decisioni di autorizzazione a policy chiaramente definite.

Inoltre, più stretta è l'integrazione tra i processi di privileged access management e gestione del ciclo di vita delle identità, maggiore è anche l'ambito a disposizione dei team di sicurezza per abilitare l'automazione su vasta scala. L'applicazione di controlli automatizzati ai ruoli e alle autorizzazioni di accesso assegnati alle identità con privilegi può consentire l'identificazione proattiva delle violazioni, come uno sviluppatore che ottiene l'accesso alle credenziali per il codice in produzione.

L'importante è che gli strumenti di privileged access management devono essere in grado di supportare l'automazione nel processo di autorizzazione e garantire la scalabilità attraverso il supporto di operations dinamiche e infrastrutture effimere, come gli account amministrativi AWS per le identità umane.

Molti degli attuali approcci al privileged access management sono incentrati sulla copertura di un sottoinsieme di identità con privilegi e non sono stati concepiti pensando all'infrastruttura IT di oggi. Per passare alle fasi successive di un maturity model, le imprese devono considerare il modo in cui gli approcci al privileged access management affrontano la proliferazione, la distribuzione e la trasformazione delle identità con privilegi, in base alla capacità di:

- Estendere la governance e la visibilità delle identità con privilegi dai data center on-premise a quelli virtualizzati, fino ai servizi cloud.
- Automatizzare l'autorizzazione dell'accesso con privilegi a partire dai requisiti operativi, attraverso l'integrazione con policy di gestione delle identità basate su ruoli, anziché tramite processi di approvazione manuali.
- Scalare e integrare controlli e monitoraggio nell'infrastruttura dinamica ed effimera.
- Agevolare la governance e il monitoraggio continuo centralizzato, per identificare i casi in cui vengono inizialmente concessi privilegi eccessivi e attivare un workflow di correzione.
- Incorporare capacità rilevamento e correzione, a mano a mano che le nuove minacce si evolvono, tramite funzioni di machine learning e modelli basate sui dati.

Sezione 4

Inquadrare il rischio nel contesto appropriato

Poiché i programmi di digital transformation danno origine a reti distribuite, cambiamenti frequenti, alti volumi di transazioni e un maggior numero di identità con privilegi, costituiscono un problema per i tradizionali approcci basati su regole al rilevamento degli usi scorretti o dei furti di credenziali con privilegi, che si sono già dimostrati inadeguati anche per le minacce esistenti.

Adottando un approccio più generalizzato all'analisi degli accessi con privilegi e inviando più dati ai sistemi SIEM (Security Information And Event Management) si perdono importanti informazioni sul contesto che permettono ad analisti della sicurezza e personale IT operativo di effettuare una distinzione critica fra incoerenze, gravi anomalie e attività ad alto rischio che richiedono una correzione.

Occorre piuttosto un approccio specifico del dominio, che utilizza le informazioni relative al contesto e la conoscenza di ruoli e comportamenti degli utenti con privilegi per trovare l'ago nel pagliaio, ovvero le azioni che costituiscono una prova concreta di un attacco, e rispondere adeguatamente.

Un approccio specifico del dominio segue gli stessi principi della definizione di una linea di base comportamentale, ovvero l'identificazione delle azioni compiute dagli utenti con privilegi, i loro comportamenti passati e il livello di rischio associato alle azioni, inclusa la sensibilità della risorsa di destinazione, e le modalità di accesso ai sistemi. Tale approccio deve tuttavia includere una relazione grafica fra le entità, per inquadrare il comportamento nel relativo contesto.

Sezione 5

Conoscere gli utenti con privilegi per conoscere i rischi

Per identificare più efficacemente gli attacchi che sfruttano il furto di credenziali non basta accumulare più dati, ma occorre incorporare dati più mirati sul comportamento degli utenti con privilegi, per consentire l'identificazione di cambiamenti significativi che possono essere il sintomo di un rischio reale.

Questo approccio viene ulteriormente rinforzato attraverso l'integrazione con sistemi di governance degli accessi con privilegi, per consentire l'analisi comportamentale tra utenti con ruoli paragonabili. Quando una macchina o un utente con privilegi accede a un sistema incoerente con il suo ruolo e il comportamento delle altre entità analoghe, oppure accede a un sistema da un indirizzo IP diverso dal solito ed esegue azioni incoerenti con i sistemi passati, il sistema può rilevare in modo più preciso se il comportamento è sintomatico di un attacco e attivare le misure appropriate.

Sezione 6:

Conclusioni

La digital transformation non avviene da un giorno all'altro, ma dipende inevitabilmente dalla capacità di automatizzare sia l'applicazione delle policy di sicurezza per le identità più a rischio, sia il rilevamento delle potenziali minacce derivanti dall'uso scorretto di itali identità con privilegi. L'implementazione di un approccio basato sui rischi garantisce controlli di sicurezza e analisi perfettamente allineati con il percorso di digital transformation, permettendo di abilitare automazione, scalabilità e velocità senza compromessi e a costi contenuti. Prima di intraprendere questo percorso occorre delineare una roadmap chiara, distribuita su più anni, che consenta di anticipare i requisiti a breve e lungo termine di una soluzione per il privileged access management, garantendo la portata e la scalabilità necessarie a un costo ragionevole per l'intero ciclo di vita.

La sicurezza costituisce un imperativo, ma la portata, la scalabilità e i costi relativi non possono rappresentare un ostacolo alla digital transformation.

Per ulteriori informazioni sui vantaggi che CA PAM può offrire al tuo business, visita il sito **ca.com/pam**

Il sito di CA Technologies è disponibile all'indirizzo ca.com/it

CA Technologies (NASDAQ: CA) crea software che promuove l'innovazione all'interno delle aziende, consentendo loro di cogliere le opportunità offerte dall'application economy. Il software rappresenta il cuore di qualsiasi business, in ogni settore. Dalla pianificazione allo sviluppo, fino alla gestione e alla sicurezza, CA Technologies collabora con le aziende di tutto il mondo per cambiare il nostro modo di vivere, interagire e comunicare, in ambienti mobile, cloud pubblici e privati, distribuiti e mainframe. Per ulteriori informazioni, visita il sito **ca.com/it**.

CS200-270334_0517