WHITE PAPER | GIUGNO 2017

Privileged access management: roadmap per calcolare il Total Cost of Ownership (TCO)

Scoprire i costi nascosti e i benefici dell'approccio di implementazione di PAM

ca technologies

Sommario

Sezione 1

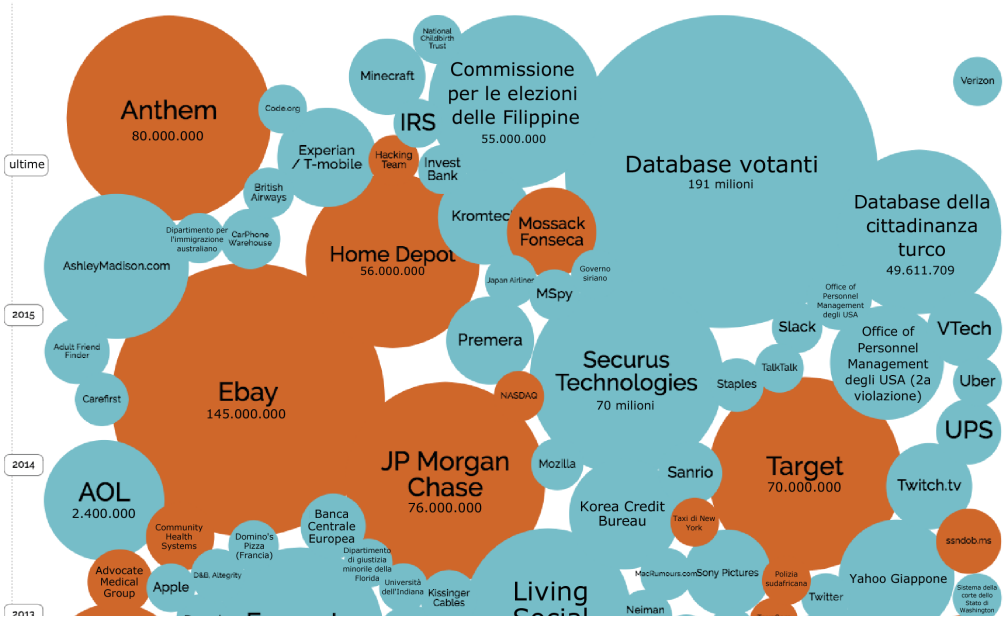
Introduzione

Gli account utente con privilegi (usurpati, violati o semplicemente utilizzati in modo scorretto) sono al centro della maggior parte delle violazioni dei dati. I team di sicurezza stanno prendendo sempre più in considerazione le soluzioni complete per il privileged access management (PAM, Privileged Access Management), per evitare i danni causati da un utente non autorizzato con privilegi elevati o da un utente con privilegi stanco, stressato o che commette semplicemente un errore e per rispondere alla richieste di dirigenti e team di audit di ridurre l'esposizione del business. Ma una soluzione PAM completa può introdurre costi nascosti, a seconda della strategia di implementazione adottata. A causa delle numerose funzionalità, che includono vault delle password, gestione e monitoraggio delle sessioni e spesso analytics sul comportamento degli utenti e l'intelligence sulle minacce, la modalità con cui viene implementata una soluzione PAM può produrre un impatto notevole su costi e benefici. Questo report fornisce un modello per la determinazione dei costi diretti, indiretti e nascosti di un deployment di PAM nel tempo.

Sezione 2

Account con privilegi collegati alle violazioni di alto profilo

Le violazioni della sicurezza di alto profilo sono ormai una costante negli annunci di cronaca e, secondo gli esperti, nell'80-100% dei casi coinvolgono l'uso di account con privilegi. Un numero sempre crescente di attacchi coinvolge gli account di amministratori IT, sviluppatori di applicazioni, business manager, partner, fornitori e dirigenti. Una volta entrato nel sistema, l'autore dell'attacco può spostarsi in orizzontale e in verticale per accedere a informazioni sensibili e installare malware per provocare danni futuri. Ma per l'amministratore IT non è sempre facile stabilire se l'accesso degli utenti con privilegi alle aree sensibili costituisce un problema, poiché potrebbe rientrare nelle loro mansioni quotidiane.



In sostanza, il ruolo dell'utente con privilegi può costituire l'anello debole della catena di sicurezza per qualsiasi azienda del mondo, indipendentemente dalle dimensioni, e affrontandolo correttamente è possibile risparmiare sui costi per molti anni a venire.

Sezione 3

Protezione dalle violazioni tramite account con privilegi con PAM

La protezione delle informazioni coinvolge molti aspetti, e uno di questi è costituito dal privileged access management. In genere le aziende prestano una notevole attenzione alle soluzioni PAM, per uno o due motivi:

- Si trovano di fronte a un problema serio (ad esempio, hanno subito una violazione o non soddisfano i requisiti di compliance)
- Sono pronte a implementare le best practice

Indipendentemente dal motivo, l'implementazione di una soluzione PAM si basa in genere su una serie di presupposti. Si può avere la tentazione di adottare una prospettiva a breve termine, presupponendo di poter iniziare con un insieme limitato di funzionalità per poi incrementare la portata e la scalabilità dell'implementazione strada facendo. Anche se questo approccio può essere ragionevole con altre misure di sicurezza, l'esperienza dimostra che, nel caso di una soluzione PAM, è sconsigliabile sia dal punto di vista tecnico che da quello economico. Infatti, in quest'area specifica è estremamente importante adottare una visione a lungo termine: device, endpoint, utenti e account devono essere protetti tenendo conto dei problemi di compliance, oltre che della roadmap aziendale. Tutti questi fattori influiscono sul Total Cost of Ownership (TCO).

Device

Proteggere gli endpoint tradizionali non basta più. Oggi l'ambito si è allargato fino a comprendere ambienti virtualizzati, container e sistemi basati su cloud. L'infrastruttura IT ibrida, le console di gestione, il numero elevato di risorse e i cambiamenti continui possono estendere la superficie di attacco disponibile. Una protezione adeguata richiede difese che incorporano l'intero ambiente fin dall'inizio, per garantire una profondità e un'ampiezza commisurate alle minacce. Quando si pianifica un'implementazione di PAM, occorre tenere presenti questo tipo di esigenze future.

Utenti

Oggi il phishing e l'ingegneria sociale sono tra i metodi più comuni per ottenere le credenziali di un utente con privilegi. Le minacce esterne (e un numero sempre crescente di minacce interne) richiedono informazioni contestuali complete, poiché per isolare le situazioni anomale è necessario comprendere il comportamento normale degli utenti con privilegi. L'adozione di cloud, ambienti ibridi e metodologie di sviluppo Agile sta trasformando il concetto stesso di utente con privilegi: ad esempio, i responsabili Line of Business possono ottenere privilegi amministrativi per le soluzioni CRM basate su cloud. Il problema è ulteriormente complicato dal fatto che il comportamento degli utenti cambia nel tempo e gli attacchi mirati si evolvono, al punto che non è facile stabilire con certezza se un account sia stato compromesso o meno. Le soluzioni di gestione degli utenti con privilegi devono migliorare costantemente, per essere in grado di identificare le potenziali violazioni.

Compliance

L'esigenza di garantire e dimostrare la compliance, che costituisce un requisito costante per aziende di ogni dimensione, può rapidamente condurre alla "stanchezza normativa" (regulatory fatigue), a causa del volume e dell'ambito dei cambiamenti delle normative.

Le tecnologie PAM devono supportare le normative che disciplinano i controlli e i processi utilizzati per garantire la cybersecurity, che possono includere la documentazione dell'accesso alle impostazioni di configurazione e ai dati privati, l'applicazione di ITIL® e la fornitura di audit trail definitivi per l'Health Insurance Portability and Accountability Act del 1996 (HIPAA), il Payment Card Industry Data Security Standard (PCI-DSS) e altre normative. La dimostrazione della compliance deve essere integrata fin dall'inizio, non aggiunta a posteriori.

Sezione 4

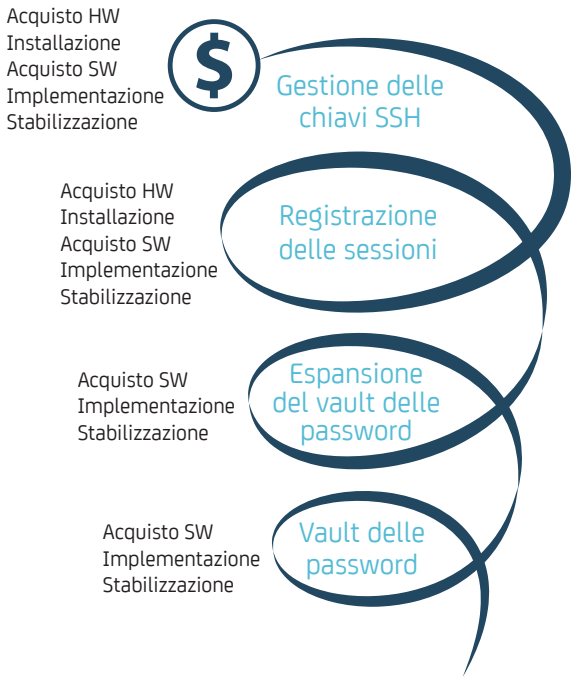
Principale impatto della strategia di implementazione di PAM sul TCO

Il metodo di implementazione scelto per una soluzione PAM produce un notevole impatto sul total cost of ownership. È importante comprendere i due metodi disponibili per l'implementazione di una soluzione PAM.

Il primo, che chiameremo "completo", consiste nel creare una roadmap dei requisiti chiave, acquistare un prodotto che fornisce fin dall'inizio tutte le capacità necessarie, inclusi i requisiti futuri, e quindi aumentare gradualmente l'ambito e la scalabilità di tali capacità nel tempo. Se ad esempio occorrono un vault delle password, la registrazione delle sessioni e la gestione delle chiavi SSH (Secure Shell), è possibile acquistare un prodotto che integra tutte queste funzionalità e attivarle a mano a mano che si rendono necessarie. Poiché sono tutte integrate, non occorre un lungo periodo di stabilizzazione.

Anche il secondo approccio, che chiameremo "graduale", inizia con una roadmap, ma i prodotti vengono acquistati al momento del bisogno. Se ad esempio la roadmap include le stesse tre capacità precedenti, è possibile acquistare prima il vault delle password e, dopo averlo implementato, stabilizzarlo per alcuni mesi, quindi tornare dal fornitore e acquistare la soluzione di registrazione delle sessioni (con tutto l'hardware aggiuntivo necessario), implementarla e stabilizzarla nell'arco di sei mesi, per poi fare lo stesso con la gestione delle chiavi SSH.

Il metodo prescelto può influire sia sul TCO che sul time-to-value. L'implementazione di una soluzione PAM completa e integrata, basata su funzionalità di raccolta dei dati di intelligence, può consentire al tempo stesso di accelerare il time-to-value e ridurre il TCO. I costi sono noti e prevedibili. Viceversa, nel caso dell'implementazione graduale, il deployment iniziale può essere semplice: un vault delle password per un numero limitato di account, che si espande con il tempo incrementando il numero degli account nel vault, seguito dall'aggiunta di una soluzione per la registrazione delle sessioni. Tuttavia, le spese possono diventare imprevedibili, perché i costi di infrastruttura possono variare con ogni modulo aggiunto. Inoltre il cliente rimane vincolato al fornitore, con tutti gli svantaggi del caso. In un'implementazione graduale i calcoli del TCO devono tenere conto del costo, del tempo e dell'esposizione risultanti dall'aumento di scalabilità e ambito. I costi possono essere sia materiali (costi di licenza, infrastruttura e simili), sia immateriali, come il time-to-value, l'esposizione prolungata al rischio, i costi di integrazione e manutenzione e così via. Ad esempio, le attività di creazione degli script e la manutenzione per gli endpoint aggiunti al vault delle password possono essere molto diverse da quelle necessarie per la gestione delle chiavi SSH.



Per farsi un'idea più chiara delle domande da porre e delle funzionalità da valutare, è necessario conoscere i vari componenti di una soluzione PAM completa, nonché imparare a determinare i vantaggi qualitativi e quantitativi in relazione ai costi finanziari.

Sezione 5

Principali elementi di una soluzione PAM completa

Una soluzione PAM completa include numerosi componenti di base, tra cui la capacità di controllare l'accesso con privilegi alle varie risorse, l'archiviazione sicura delle credenziali con privilegi, il monitoraggio e la registrazione delle attività, la protezione di console di cloud ibrido e gestione API, nonché l'analisi del comportamento degli utenti al fine di rilevare anomalie che potrebbero essere un sintomo di compromissione. Ecco alcuni aspetti specifici da tenere presenti durante la valutazione di una soluzione PAM:

Vault delle password. Un vault delle password (o archivio sicuro) altamente protetto e crittografato per l'archiviazione delle credenziali consente di gestire le password e le altre credenziali o token, modificandole a intervalli configurabili in base alle policy. Questo consente di proteggere gli account amministrativi, condivisi e di servizio, oltre agli account da applicazione ad applicazione e agli ambienti cloud ibridi. Tuttavia, il vault delle password da solo non è sufficiente.

Monitoraggio delle sessioni. Questo componente essenziale è spesso il grande assente durante la fase iniziale di un deployment graduale. La possibilità di avviare automaticamente una sessione remota che registra, analizza e monitora una sessione utente con privilegi consente il monitoraggio in tempo reale e l'analisi della sessione a posteriori. Questa funzionalità non dovrebbe essere aggiunta in un secondo momento: quando un utente con privilegi viola una policy o comunque manifesta un comportamento anomalo, occorre iniziare a monitorarlo immediatamente, non a distanza di sei mesi.

Ambienti ibridi. Una soluzione PAM completa è in grado di controllare l'accesso con privilegi a risorse cloud, macchine virtuali e hypervisor, oltre ai tradizionali ambienti di data center fisici. Il rilevamento automatico è fondamentale, perché bastano pochi minuti per aggiungere nuove risorse all'ambiente.

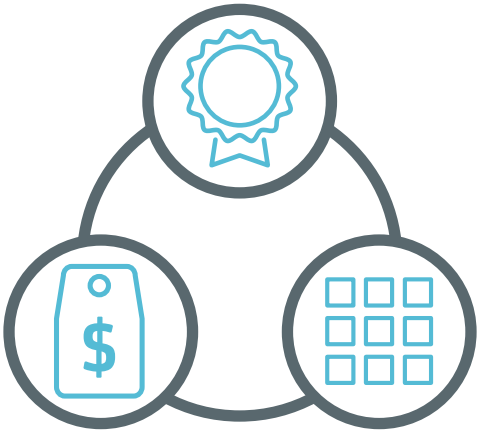
Analisi del comportamento degli utenti. Una soluzione PAM completa è in grado di distinguere le anomalie dal comportamento normale degli utenti con privilegi e attivare meccanismi di protezione aggiuntivi quando rileva attività insolite. Raccoglie dati contestuali specifici del dominio ed esegue analisi avanzate per definire modelli di rischio basati sugli schemi di comportamento precedenti. Quando rileva un comportamento insolito, può attivare automaticamente funzioni di autenticazione aggiuntive (quali Radius, TACACS+ o CA Advanced Authentication) o la registrazione delle sessioni.

Oltre a fornire queste capacità, una soluzione PAM completa è anche veloce da implementare, fornisce informazioni dettagliate e funzionalità di rilevamento out-of-the-box e richiede competenze specialistiche minime per ottenere vantaggi immediati. Consente agli amministratori di indagare agevolmente sugli incidenti e comprendere la modalità di utilizzo degli account con privilegi.

Sezione 6

Valutazione dell'impatto sul business di una soluzione PAM completa per l'azienda

Ma, alla luce di questi requisiti, quali sono i fattori importanti per determinare costi e benefici? Ad alto livello, è necessario valutare tre tipi di fattori, ovvero costi finanziari, vantaggi qualitativi e vantaggi quantitativi. I vantaggi quantitativi sono relativamente facili da identificare, basandosi sulle medie di settore e sulle procedure specifiche dell'azienda. I vantaggi qualitativi sono un po' più difficili da misurare, ma aspetti come i tempi di rilevamento delle minacce, la semplicità di utilizzo e altri fattori simili possono avere un impatto determinante. Nelle successive sezioni viene spiegato come affrontare ciascuno di questi aspetti.



Fattori da considerare per il calcolo dei costi finanziari

Il calcolo dei costi finanziari è in genere un semplice esercizio, che include:

- Costi di licenza dei prodotti (una tantum, abbonamento)
- Costi di manutenzione dei prodotti (seconda fase e oltre, costi di supporto interni)
- Costi di deployment dei prodotti (servizi professionali, deployment, configurazione)
- Costi di formazione (formazione dei clienti internali, formazione degli utenti finali)

Nel calcolo dei costi finanziari occorre tenere conto di vari problemi. Innanzitutto, il costo di implementazione di una soluzione completa rispetto a quello di un'implementazione graduale. Nel caso di una soluzione completa, è necessario tenere in considerazione il costo iniziale (che include licenze, deployment e formazione) e tutti i costi di manutenzione successivi. Per un'implementazione graduale, invece, il calcolo deve includere anche il costo dell'integrazione, che può essere direttamente proporzionale al numero e alle dimensioni dei sistemi da integrare. Se si decide di acquistare una soluzione PAM in più fasi, anziché tutta insieme, occorre prevedere costi di acquisto, formazione e deployment incrementali, in aggiunta ai costi di base indicati sopra. Anche le spese operative (OPEX) costituiscono un fattore importante nella scelta dell'implementazione graduale: le capacità aggiuntive spesso richiedono hardware dedicato, che deve essere incluso nel budget, acquistato, configurato e gestito. Quando si sceglie un approccio graduale, nel calcolo dei costi occorre anche tenere conto delle risorse, del tempo e delle competenze necessari, e questo alto numero di incognite costituisce un problema concreto durante la definizione del budget.

Fattori da considerare nella determinazione dei vantaggi economici qualitativi

I vantaggi economici qualitativi possono essere molto difficili da valutare, ma giocano un ruolo determinante quando si tratta di scegliere tra una soluzione completa e un'implementazione graduale. Consideriamo innanzitutto l'implementazione graduale: si inizia con un vault delle password per un numero limitato di account, con il tempo si aggiungono ulteriori account con privilegi, successivamente la registrazione delle sessioni e infine, terminata l'implementazione dell'intero sistema, si considera l'analisi del comportamento degli utenti.

Pro:

- I costi iniziali sono in genere inferiori

Contro:

- Il time-to-value è decisamente superiore: non è possibile ottenere visibilità con una velocità sufficiente a contenere efficacemente i rischi
- Rischio notevolmente superiore in caso di violazione: l'implementazione dell'hardware necessario per funzionalità come la registrazione delle sessioni può introdurre settimane o mesi di ritardo
- Aumento della superficie esposta per lunghi periodi di tempo
- Può richiedere la creazione di codice o script per scalare l'implementazione
- Costi aggiuntivi per hardware, backup e ridondanza: i costi a lungo termine sono in genere superiori
- Dipendenza dal fornitore: ogni volta che si prende in considerazione un nuovo modulo, il processo di approvvigionamento ricomincia e i tempi di attesa per i moduli successivi potrebbero ripartire da zero, determinando tempi di attesa dei prodotti superiori a quelli previsti inizialmente

Una soluzione completa, integrata e perfettamente funzionale, da implementare in un singolo passaggio, richiede invece la capacità di scegliere fin dall'inizio una soluzione con tutte le funzioni necessarie. Anche se è possibile attivare le funzionalità quando necessario, tutto deve essere pronto in qualsiasi momento. Questo tipo di implementazione, soprattutto se viene fornito sotto forma di appliance, garantisce il contenimento dei rischi out-of-the-box e consente di ottenere vantaggi immediati senza richiedere competenze specialistiche. Questo riduce il carico di lavoro e al tempo stesso evita le violazioni.

Pro:

- Veloce da implementare, time-to-value rapido
- Protezione immediata in caso di sospetta violazione: se è necessaria la registrazione delle sessioni, basta attivarla
- Le funzionalità aggiuntive, come l'analisi, sono immediatamente disponibili per garantire controllo e visibilità su tutto l'ambiente
- Superficie di attacco notevolmente ridotta
- Costo totale inferiore: non è necessario creare codice o script personalizzati, né hardware aggiuntivo

Contro:

- I costi iniziali possono essere superiori

I vantaggi economici qualitativi possono essere influenzati anche da alcuni fattori tecnologici. Se la soluzione PAM usa l'analisi del comportamento degli utenti e la stretta integrazione con l'intelligence sulle minacce, la capacità di rilevare le attività anomale e intervenire immediatamente è notevolmente superiore. Se la soluzione dispone di clustering multi-sito, può garantire una disponibilità superiore e tempi di risposta più rapidi. Se la soluzione viene fornita sotto forma di appliance virtuale o fisica, i tempi di implementazione sono molto più brevi, rispetto a una soluzione basata sul software. Infine, è importante tenere conto dei costi di manutenzione, che per un'appliance possono essere notevolmente inferiori a quelle di una suite di prodotti software, ciascuno dei quali richiede un componente hardware dedicato.

In sintesi, tutti i precedenti fattori qualitativi possono contribuire a ridurre il total cost of ownership (TCO) e ad accelerare il time-to-value.

Fattori da considerare nella determinazione dei vantaggi economici quantitativi

Per quanto riguarda i vantaggi economici quantitativi, è necessario considerare tre fattori chiave, ovvero la riduzione dei costi, l'aumento di produttività e la protezione dei ricavi.

Riduzione dei costi

La riduzione dei costi include l'eliminazione dei costi di infrastruttura, dei costi correlati alle violazioni, degli onorari degli auditor, dei costi di compliance e dei costi delle interruzioni di servizio non pianificate. Un altro fattore da non sottovalutare è rappresentato dalla riduzione dei costi di deployment, manutenzione e supporto.

I costi di infrastruttura possono essere evitati scegliendo una soluzione PAM completa basata su appliance, anziché una soluzione graduale o solo software. Per eseguire questo calcolo, occorre stimare il numero di server/appliance necessari per una soluzione PAM esistente o concorrente, il costo per server, il numero delle utilità di bilanciamento del carico necessarie e il costo di ciascuna, nonché la percentuale dei costi di infrastruttura che potrebbero essere evitati con una soluzione basata su appliance.

I costi correlati alle violazioni includono le perdite di profitti, i costi di notifica ai clienti, i costi di risposta agli incidenti e delle pubbliche relazioni, oltre agli onorari dei legali. Per calcolare questi costi è necessario stimare la probabilità di una violazione (la stima attuale è del 22% nell'arco di due anni), il volume dei record potenzialmente esposti e il costo per record, oltre al costo della correzione e alla percentuale di tali costi che potrebbe essere evitata con una soluzione PAM completa. Poiché si valuta che oltre l'80% delle violazioni sia dovuta alla compromissione delle credenziali, i vantaggi possono essere notevoli.

Gli onorari degli auditor esterni e i costi di compliance possono essere ridotti utilizzando una soluzione PAM completa. Per calcolare la possibile riduzione, occorre stimare il numero dei potenziali problemi di compliance l'anno, il costo annuale delle violazioni della compliance, l'onorario dell'auditor esterno per la correzione di un problema dichiarabile e la percentuale dei costi correlati ai risultati degli audit, alla correzione e alle sanzioni per problemi di compliance che potrebbero essere evitati utilizzando una soluzione PAM completa.

Un altro potenziale vantaggio è costituito dalla riduzione della probabilità degli arresti non pianificati dei sistemi, che potrebbero determinare l'insoddisfazione o un calo di produttività dei dipendenti e potenzialmente un aumento del tasso di abbandono dei clienti. Il calcolo include una stima del numero delle potenziali interruzioni di business l'anno dovute alla violazione di account utente con privilegi, del downtime medio per arresto dei sistemi, del costo al minuto e dell'impatto della maggiore disponibilità.

Uno dei principali problemi correlati al deployment graduale di una soluzione PAM è rappresentato dal fatto che i costi di manutenzione e implementazione aumentano notevolmente con ogni modulo acquistato, implementato e stabilizzato. Sono necessarie competenze specifiche per la creazione degli script, ma non tutti i clienti sono disposti ad assumere una persona a tempo pieno da dedicare alla gestione, alla manutenzione e al deployment della soluzione. Tale costo può essere evitato acquistando una soluzione completa e quindi implementando le varie funzionalità a mano a mano che diventano necessarie.

Aumento della produttività

L'aumento della produttività si manifesta in due modi, ovvero la riduzione dei costi di manodopera dell'amministratore dei sistemi IT e la riduzione dei costi operativi di implementazione e applicazioni.

Una soluzione PAM completa permette di ridurre il tempo dedicato dall'amministratore di sistema al rilevamento, all'applicazione delle policy, al recupero o alla rigenerazione delle password, oltre che di aumentare il tempo disponibile per l'implementazione di soluzioni innovative per l'evoluzione del business. Per calcolare la riduzione dei costi di manodopera dell'amministratore dei sistemi IT, è necessario considerare il numero di risorse e device con credenziali di accesso con privilegi e il numero degli account per risorsa, device o app. Occorre quindi determinare il numero di minuti necessario a un amministratore IT per fornire o aggiornare l'accesso con privilegi e il costo orario medio caricato, oltre alla riduzione prevista del tempo di aggiornamento delle credenziali di accesso con privilegi tramite la soluzione PAM completa.

I costi operativi e di implementazione possono essere drasticamente ridotti tramite una soluzione PAM completa basata su appliance. Per calcolare tale risparmio, occorre considerare il numero degli amministratori dei sistemi IT necessari per implementare, ospitare e gestire una soluzione esistente o concorrente e il relativo costo orario medio caricato l'anno, quindi applicare la riduzione percentuale dei costi che ci si può aspettare quando si sceglie una soluzione PAM completa basata su appliance.

Protezione dei ricavi

Una soluzione PAM completa può fare molto per limitare le conseguenze economiche più gravi di una violazione dei dati. Per calcolare questo vantaggio economico, occorre stimare il potenziale impatto sui profitti di un danno all'immagine del brand dovuto a una violazione dei dati o dei sistemi e la percentuale di protezione dei ricavi ottenibile grazie alla riduzione del rischio di compromissione delle credenziali. Da un recente report di Ponemon Institute emerge che, per le grandi imprese statunitensi intervistate nel 2016, l'impatto finanziario sui profitti dovuto al calo di reputazione del brand e alla riduzione dell'avviamento era di 3,97 milioni di dollari l'anno, pertanto una soluzione PAM è in grado di produrre un notevole impatto economico.

Sezione 7

Un approccio unitario

La necessità di adottare una soluzione PAM completa è evidente e il metodo di calcolo del total cost of ownership (TCO) deve tenere conto di una lunga serie di fattori. I costi variano a seconda che si decida di implementare una soluzione PAM completa, abilitando le funzioni a mano a mano che sono necessarie, oppure un'implementazione graduale, dopo aver determinato esattamente i costi futuri. Rivediamo quindi i costi e i benefici di un approccio completo:

- I costi sono prevedibili e facili da inserire nel budget, senza spese aggiuntive associate all'approccio graduale (approvvigionamento, licenze, formazione, deployment, risorse e infrastruttura aggiuntiva)
- I vantaggi qualitativi sono considerevoli: implementazione e time-to-value rapidi, protezione immediata in caso di violazione, superficie di attacco ridotta e TCO inferiore
- Anche i vantaggi quantitativi sono impressionanti: è possibile eliminare i costi di infrastruttura, ridurre i costi correlati alle violazioni e quelli associati ad audit e compliance, evitare le interruzioni di servizio non pianificate e ridurre i costi di deployment, manutenzione e supporto

Naturalmente, i risultati di tali calcoli variano a seconda della situazione e delle preferenze aziendali, ma è chiaro che un approccio di implementazione completo consente di ottenere un TCO molto più favorevole, rispetto a un approccio graduale all'implementazione PAM.

Sezione 8

Conclusione: una visione a lungo termine del TCO

L'estensione delle superfici di attacco non protette aumenta di giorno in giorno, incrementando il rischio per l'azienda. Una soluzione PAM completa può ridurre la superficie di attacco e garantire un time-to-value rapidissimo, un aspetto estremamente importante se l'azienda è a rischio di violazione. Questo tipo di soluzione fornisce tutte le capacità richieste fin dal primo giorno. Anche se è possibile scegliere di abilitare inizialmente solo un sottoinsieme di funzioni, quando si sospetta una violazione è possibile contare all'istante sulla potenza completa della soluzione. Esaminando i risultati dei calcoli è evidente che, a lungo termine, una soluzione PAM completa basata su appliance produce vantaggi a livello economico, di business e di produttività.

Per saperne di più sui vantaggi delle soluzioni CA privileged access management, visita il sito **ca.com/pam**

ca technologies

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**.

1 Thomson Reuters, "Cost of Compliance 2016", https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2016.html

2 Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis", giugno 2016, https://securityintelligence.com/media/2016-cost-data-breach-study/

3 Ibid.

CS200-282765_0617