WHITE PAPER | APRILE 2016

Chiudere le backdoor di rete

Cinque best practice chiave per controllare i rischi collegati all'accesso di terze parti

Dale R. Gardner
CA Security Management

ca technologies

Sommario

Executive summary

La sfida

Le importanti violazioni subite di recente da Target, Home Depot, eBay, l'Office of Personnel Management statunitense e altri soggetti sono state rese possibili dalla sottrazione o dalla compromissione di credenziali appartenenti a un utente con privilegi, dotato di ampio accesso a sistemi sensibili. In quasi due terzi dei casi, la violazione iniziale è stata facilitata dalle pratiche di sicurezza eccessivamente lasche di un terzo, un fornitore o un partner di business che aveva avuto accesso a una rete interna. Armati delle credenziali sottratte al partner, gli autori di attacchi hanno analizzato l'infrastruttura IT violata alla ricerca di account con privilegi che sono stati poi utilizzati per ottenere un accesso non autorizzato ai sistemi critici, causando gravi danni ai business.

L'opportunità

Sono numerose le aziende, analogamente a quelle vittime di queste violazioni, che si trovano a dover gestire una frustrante e complessa combinazione di fornitori, consulenti e partner di business dotati di accesso di rete alla loro infrastruttura IT, con una varietà di account con privilegi utilizzati per eseguire le applicazioni mission-critical. Nel panorama del lavoro odierno, altamente interconnesso, l'accesso non può essere completamente bloccato, e pensare di eliminare gli account con privilegi non è possibile; l'unica opzione, quindi, resta quella di proteggere meglio gli account con privilegi dagli utenti non autorizzati, migliorando così la tutela delle risorse sensibili.

I vantaggi

Risparmi sui costi di outsourcing, miglioramento della qualità ed efficienze sono tutti vantaggi alla portata dell'impresa interconnessa. Limitare l'accesso alla rete per tutti a livello di firewall non è più un'opzione. Le risorse rilevanti devono essere disponibili ai partner di business perché i vantaggi di business possano diventare realtà. È necessario implementare le best practice di sicurezza delle informazioni per bloccare le violazioni ma anche, al contempo, per consentire le attività di business legittime.

Sezione 1

Rischi generati dall'accesso di terze parti

Nella maggioranza delle aziende esiste oggi un insieme di utenti non dipendenti con un certo livello di accesso con privilegi alle reti e ai sistemi interni. Spesso, il team aziendale incaricato della sicurezza delle informazioni sa poco o nulla di questi soggetti, se non che lavorano per fornitori della società, fornitori di servizi in outsourcing o partner di business. In genere, questi utenti rappresentano il principale rischio per l'impresa, perché i loro account sono spesso la via più facile per comprometterla. I fatti di cronaca relativi a Target, Home Depot e altri sono tra gli esempi di queste violazioni. Un accesso utente di terze parti relativamente limitato può essere adottato per ottenerne uno più ampio alle reti e ai sistemi dell'azienda, con danni conseguenti di impatto enorme. Questi casi non sono eccezioni. Secondo Troy Leach del PCI Council, circa il 65% delle violazioni può essere fatto risalire a un soggetto terzo.

Gli organismi di controllo sono consapevoli di questi rischi e stanno lavorando con gli operatori del settore per sviluppare controlli e normative adeguati ad affrontare questa sfida. Ad esempio, PCI versione 3 del Data Security Standard ha introdotto nuovi controlli volti a gestire proprio il rischio collegato ai soggetti terzi. Secondo Benjamin Lawsky, sovrintendente ai servizi finanziari per lo Stato di New York, **"La cybersecurity di un'azienda spesso è legata a doppio filo a quella dei suoi fornitori. Purtroppo, queste aziende terze possono rappresentare un ingresso backdoor agli hacker che cercano di sottrarre dati sensibili dei clienti del settore bancario".** Di conseguenza, le autorità di controllo per servizi finanziari, sanità e altri settori stanno sviluppando nuovi requisiti di compliance per ridurre i rischi e migliorare la sicurezza.

> "La cybersecurity di un'azienda spesso è legata a doppio filo a quella dei suoi fornitori. Purtroppo, queste aziende terze possono rappresentare un ingresso backdoor agli hacker che cercano di sottrarre dati sensibili dei clienti del settore bancario".
>
> - Benjamin Lawsky, sovrintendente ai servizi finanziari per lo Stato di New York

---

Sezione 2

Cinque best practice chiave per controllare i rischi collegati all'accesso di terze parti

Guardando al futuro, controllare e gestire l'accesso di terze parti alle reti e ai sistemi sta diventando un requisito sempre più importante, a livello di gestione del rischio di sicurezza e di compliance normativa.

> "Gli hacker sono riusciti ad accedere alle reti di OPM tramite credenziali sottratte a un subappaltatore, KeyPoint Government Solutions".
>
> Esclusiva: I dettagli riservati della violazione subita da OPM, 21 agosto 2015

Best practice 1: implementare processi e controlli di supporto

Come per la maggior parte dei problemi di sicurezza delle informazioni, un buon punto di partenza è la definizione di processi e controlli che contribuiscano a gestire il rischio. Questo è particolarmente importante per la gestione del rischio collegato a terzi, perché la maggioranza delle attività si verifica al di fuori della competenza e del controllo diretti del team incaricato della sicurezza delle informazioni. Dato che è possibile che vengano instaurate relazioni di business e che venga fornito l'accesso ai sistemi all'insaputa e senza la supervisione del team, quest'ultimo deve essere coinvolto nelle trattative con i vendor, in modo da poter sviluppare e applicare policy adeguate come parte del framework generale di Identity and Access Management dell'azienda.

La parte semplice del processo è costituita da provisioning, de-provisioning e definizione di policy adeguate per gli utenti con privilegi che non siano dipendenti. Come per altre categorie di utenti con privilegi, è necessario definire i seguenti ambiti:

- Definizione e formazione degli utenti
- Sistemi e risorse cui è necessario accedere
- Livello di privilegi necessario per svolgere le mansioni di ciascuno
- Eventuali limitazioni da applicare
- Frequenza di monitoraggio, registrazione delle sessioni, avvisi e revisione delle sessioni

Nella maggioranza delle aziende questo tipo di policy sono già in atto per gli utenti con privilegi. Se così non è, sarà necessario crearle. Gli stessi processi e controlli che si applicano agli utenti con privilegi dipendenti devono applicarsi anche ai non dipendenti. In base alla struttura e alle dimensioni dell'azienda, a gestire questi processi saranno in genere Operations IT, singoli individui responsabili dell'Identity management, o un gruppo incaricato di gestire i contratti con i vendor. Questi gruppi devono anzitutto essere informati e concordare sui processi per la formazione, il provisioning, il monitoraggio e il deprovisioning degli utenti con privilegi terzi.

Standard di sicurezza

In linea generale, la sicurezza è robusta quanto il suo anello più debole. Attraverso l'utente con privilegi di un partner, l'infrastruttura e i processi del partner stesso diventano parte dell'infrastruttura IT di un'azienda. Un solo partner con controlli o un livello di sicurezza carente può rappresentare una via di accesso perché gli hacker violino la sicurezza dell'azienda, come dimostra la violazione ai danni dell'Office of Personnel Management, verificatasi a partire da credenziali sottratte al subappaltatore KeyPoint Government Solutions. Dal punto di vista della gestione del rischio, quindi, la valutazione della sicurezza di ogni partner a fronte degli standard definiti dall'azienda è imprescindibile. In un numero crescente di casi, PCI, HIPAA e altre normative prescrittive in materia di compliance impongono valutazioni della performance dei vendor terzi e delineano requisiti specifici.

Nella maggioranza delle aziende esistono già standard di sicurezza delle informazioni definiti: questi stessi standard devono applicarsi anche ai fornitori terzi. Per sviluppare nuovi standard di sicurezza delle informazioni sono disponibili varie fonti:

- Shared Assessments pubblica un documento SIG (Standard Information Gathering), per facilitare la standardizzare del processo di valutazione e raccolta relativo alla sicurezza delle informazioni
- L'Office of the Comptroller of the Currency (OCC) pubblica un'ampia guida informativa sulla gestione del rischio, con sezioni specifiche dedicate all'IT
- Il Federal Financial Institutions Examination Council (FFIEC) pubblica documenti che includono standard in questo ambito
- Strumento di valutazione del rischio per la sicurezza del Department of Health and Human Services
- 800-53 Security and Privacy Controls for Federal Information Systems del NIST

- Organismi regolamentari statali
- Framework di controllo e policy ISO 27002 o COBIT

Inoltre, obblighi di compliance specifici di settore possono includere requisiti applicabili alla collaborazione con soggetti terzi:

- Standard per la sicurezza dei dati PCI
- HIPAA HITECH

Implementazione, formazione e applicazione

Una volta definite, valutazioni e procedure dovranno essere implementate e applicate da IT, finanza, affari legali e dalle business unit responsabili dei rapporti con i vendor, nel contesto della normale definizione ed esecuzione dei contratti con i soggetti terzi. Di seguito vengono illustrati gli elementi di base da includere in ogni contratto con terze parti:

- Garanzie: riferimenti alle policy e alle procedure effettive che il vendor si impegna ad applicare, inclusi controllo dei precedenti e formazione dei dipendenti del vendor che accedono ai sistemi aziendali.
- Mezzi correttivi: sanzioni pecuniarie per mancata compliance e processi correttivi.
- Previsioni in materia di audit: controlli e valutazioni disponibili per convalidare la compliance e la frequenza di audit.

Queste condizioni essenziali per la gestione del rischio devono essere integrate nelle fasi rilevanti del processo di negoziazione e di esecuzione. I dettagli relativi a policy e loro applicazione varieranno per le diverse aree di business, nell'ottica di un bilanciamento tra rischi e costi.

Best practice 2: autenticare meglio gli utenti

La principale opportunità di mitigazione del rischio, che consente costo e sforzo minimi a fronte di una riduzione del rischio massima, è rappresentata dall'identificazione e dall'autenticazione degli utenti. Come accennato in precedenza, circa due terzi delle violazioni possono essere ricondotti a un'identificazione e un'autenticazione insufficienti degli utenti terzi, inclusa la gestione delle credenziali (o la sua assenza). In generale, le aziende terze tendono ad essere imprese più piccole, che mancano della maturità e dell'esperienza, nell'ambito della sicurezza, tipiche delle entità di maggiori dimensioni. Questo, spesso, genera problemi. Le credenziali utente possono essere compromesse in due modi: a causa di un livello di robustezza e di una gestione delle credenziali inadeguati, o della divulgazione involontaria delle credenziali alla persona sbagliata.

- **Credenziali non sicure:** anche qualora venga selezionata una password complessa, far rispettare le regole relative alle password e alla loro scadenza può essere un processo ripetitivo e sgradevole; le persone, i vendor minori in particolare, non seguono queste regole. Pensiamo ad esempio a un fornitore terzo che usa le stesse credenziali per tutti i clienti. Una volta compromesso quel set di credenziali per un cliente, l'autore di un attacco potrebbe semplicemente far passare l'elenco dei clienti del fornitore (comodamente disponibile sul suo sito web) e andare a colpirli tutti, uno per uno.
- **Divulgazione errata:** secondo statistiche recenti, la percentuale di successo dei tentativi di phishing ripetuti è vicina al 100%, dopo appena 5-7 tentativi. Questo è una conseguenza del livello di complessità raggiunto da questi tentativi, e del fatto che anche gli utenti più esperti e sofisticati sono e restano fallibili. Per compromettere l'azienda basta un solo errore, come dimostra la violazione della rete elettrica ucraina verificatasi nel mese di dicembre 2015. Questo significa che anche partner di business esperti possono rimanere vittime di attacchi di phishing.

Il modo migliore per proteggere le credenziali di accesso ai sistemi consiste nel gestirle e controllarle in modo proattivo, con definizione e applicazioni di policy, tra le quali

- Complessità
- Frequenza delle modifiche
- Autenticazione multifattore

Una best practice per la gestione delle credenziali è l'autenticazione multi-fattore per tutti gli utenti di terze parti (e per gli utenti con privilegi interni). Quando un'azienda viene presa di mira, è solo questione di tempo prima che le credenziali utilizzate da un vendor terzo vengano violate. Ad esempio, nel caso della violazione della rete elettrica ucraina, sembrerebbe che il malware BlackEnergy sia stato inviato a un utente con privilegi ignaro tramite allegato infetto di Microsoft Office, e quindi utilizzato come vettore di accesso iniziale per acquisire le credenziali legittime. Il modo migliore per impedire questo tipo di situazioni consiste nell'aggiungere un ulteriore fattore al processo di autenticazione. Le opzioni per l'autenticazione multi-fattore disponibili sono diverse. L'opzione più efficace nello specifico dipende da una combinazione di fattori economici e di normative o requisiti di compliance. Ad esempio, nell'ambito del governo federale degli Stati Uniti, esistono requisiti specifici per l'utilizzo di carte PIV/CAC da parte degli utenti con privilegi e amministrativi. In altri ambienti sono disponibili alternative diverse, come certificati, token basati su hardware o software, oppure processi di verifica che utilizzano il telefono cellulare dell'utente. L'aspetto economico dell'autenticazione multi-fattore risulta molto favorevole, facilitando la creazione del caso di business.

Un'efficace gestione delle credenziali di terze parti si basa sull'assegnazione agli utenti del vendor di credenziali individuali, cosa che le pratiche di business correnti di molte aziende non prevedono. In molti casi, anziché creare un account per ogni utente, viene creato un account per il fornitore, con l'intesa che ciascuno dei suoi dipendenti potrà utilizzare lo stesso account e le stesse credenziali. Anche se può risultare più facile da un punto di vista amministrativo, la condivisione di un account da parte di più persone determina una serie di problemi:

- L'autenticazione multi-fattore è ovviamente più complessa.
- Risulta più difficile controllare l'accesso e l'utilizzo delle credenziali, in particolare quando qualcuno lascia l'azienda o il suo ruolo si modifica. La divulgazione o la sottrazione delle credenziali condivise è davvero troppo semplice.
- Diventa impossibile l'attribuzione, ovvero la capacità di determinare chi ha eseguito una particolare operazione sulla rete. Se un account è condiviso tra più persone, non c'è modo di sapere quale di questi individui ha eseguito l'operazione problematica.

L'implementazione di un processo in cui le credenziali vengono rilasciate a singoli, piuttosto che al vendor, elimina gran parte di questi problemi e semplifica il processo di on-boarding e off-boarding degli utenti. Quando un soggetto entra a far parte dell'organico di un partner di business, viene creato un account e viene fornito l'accesso, che verranno poi rimossi, con altrettanta facilità e rapidità, quando la persona lascia l'azienda o cambia mansioni. Una gestione degli accessi e un'autenticazione utente corrette non sono solo problematiche dal punto di vista tecnologico, ma presentano difficoltà che coinvolgono anche persone, processi e formazione, da affrontare al momento della negoziazione dei contratti con i vendor e della definizione dei processi. Non solo i vendor devono comunicare le modifiche apportate al proprio organico (il che rappresenta per loro lavoro extra), ma devono anche esistere procedure per facilitare il reporting di questi eventi da parte loro. Nel complesso, lo sforzo amministrativo supplementare vale decisamente la maggiore sicurezza e il maggiore controllo che questi approcci forniscono. In effetti, i requisiti normativi impongono l'autenticazione e il controllo degli accessi a livello individuale, proprio per la loro efficacia.

L'ultimo ambito, che può essere poco diffuso all'interno delle aziende, è costituito dall'imporre il controllo dei precedenti e la prova dell'identità agli individui terzi che accedono ai sistemi dell'azienda. Anche questo è un problema di gestione del rischio: il costo (finanziario e amministrativo) di queste procedure è generalmente giustificato, soprattutto in ambienti sensibili.

Una tecnologia che centralizza e automatizza le regole di complessità delle password, le modifiche delle password stesse e l'integrazione di sistemi di autenticazione multi-fattore è rappresentata dall'archivio delle credenziali. Dopo la gestione delle credenziali, il componente più accessibile è sicuramente la separazione dell'autenticazione dal controllo degli accessi.

Best practice 3: separare l'autenticazione dal controllo degli accessi

Nella maggioranza delle infrastrutture, una volta acquisito l'accesso alla rete, il soggetto ha visibilità, e potenzialmente accesso, a una vasta gamma di device e sistemi. Tra le conseguenze di questa architettura di rete ci sono violazioni come quelle subite da Target, Home Depot, la rete elettrica ucraina e molti altri. Esse vengono realizzate utilizzando una kill chain di violazione. Mediante questo metodo, gli autori di attacchi eseguono una serie di passaggi, a volte in modo iterativo, per portare a termine con successo una violazione. L'attacco inizia ottenendo l'accesso iniziale a una rete, spesso attraverso credenziali compromesse di un vendor o di un terzo. Una volta all'interno della rete, gli hacker possono andare alla ricerca di vulnerabilità e altre credenziali da utilizzare per ampliare ulteriormente l'accesso, con privilegi di livello sempre più elevato, come è successo nel caso delle violazioni subite da Target, Home Depot e la rete elettrica ucraina.

> "Tutte e tre le aziende hanno indicato che gli autori dell'attacco avevano rimosso il contenuto di alcuni sistemi eseguendo il malware KillDisk a conclusione dell'attacco. Il malware KillDisk elimina file selezionati sui sistemi di destinazione e danneggia il master boot record, rendendo i sistemi inutilizzabili. È stato inoltre segnalato che, almeno in un caso, sono state sovrascritte utilizzando KillDisk anche interfacce uomo-macchina (HMI) basate su Windows integrate nelle unità terminali remote. Gli autori dell'attacco hanno reso inutilizzabili anche device Serial-to-Ethernet presso sottostazioni, danneggiandone il firmware. In aggiunta, hanno apparentemente pianificato la disconnessione dei gruppi di continuità (UPS) dei server tramite l'interfaccia di gestione remota degli UPS stessi. Il team valuta che queste azioni sono state eseguite nel tentativo di interferire con gli interventi di ripristino attesi".
>
> Attacco informatico contro l'infrastruttura critica ucraina
> Data di pubblicazione originale: 25 febbraio 2016

Come accennato nella sezione dedicata alla best practice 2, un modo per interrompere la kill chain consiste nel controllare l'accesso alla rete e rendere più difficile l'ingresso a un utente malintenzionato, utilizzando l'autenticazione multi-fattore. Un altro livello di difesa è rappresentato dal limitare la visibilità e l'accesso alle risorse di rete dell'utente medesimo. La maggioranza dei vendor ha necessità di accedere solo a sistemi molto specifici. Non è necessario che dispongano dell'accesso e nemmeno della visibilità su tutta la rete, o su una sottorete.

La visibilità e l'accesso alla rete possono essere limitati mediante la segmentazione di rete fisica, che viene spesso implementata per adeguarsi a obblighi normativi. Segmentando la rete e controllando l'accesso, l'ambito delle risorse disponibili può essere limitato. Questo approccio, potenzialmente efficace, presenta però anche degli svantaggi:

- Sovraccarico eccessivo per la configurazione e la gestione dell'architettura di rete
- Vulnerabilità collegate alle connessioni tra le diverse parti della rete: l'autore di un attacco può trovare un modo per utilizzare le connessioni di rete e ottenere l'accesso al proprio obiettivo

Un'alternativa migliore consiste nell'utilizzare la segmentazione logica con una soluzione di Privileged Identity Management, come ad esempio CA Privileged Access Manager, in grado di limitare l'accesso alle risorse. Questa soluzione funziona mediante l'implementazione di un "punto di strozzo" che l'utente terzo deve superare per ottenere l'accesso alle risorse protette. Tale approccio si traduce in una serie di vantaggi:

- **Controllo degli accessi Zero Trust:** anche dopo aver eseguito il login con successo, non si ottiene accesso a tutta la rete. Vengono invece applicate dal sistema policy che specificano quali risorse sono disponibili a un utente, limitandone l'accesso solo a quei sistemi. Questo approccio consente un controllo molto rigoroso della visibilità e dell'accesso: l'individuo nemmeno vede le risorse cui non è autorizzato ad accedere, i suoi privilegi anche in lettura si limitano all'elenco predefinito di sistemi per i quali è autorizzato.
- **Prevenzione del movimento leapfrog:** per controllare il movimento laterale all'interno di una rete, il sistema intercetta una varietà di comandi di rete, come TELNET o SSH, e ne impedisce l'esecuzione. Questa capacità limita l'accesso dei terzi solo a sistemi specificati a priori, eliminando modi potenziali per ottenere visibilità sul resto della rete e tentare di raggiungere altri sistemi.

È importante standardizzare e consolidare i metodi di accesso con un punto di strozzo, utilizzando una soluzione di Privileged Access Management, una VPN o altra soluzione che incanali l'accesso su percorsi conosciuti. La definizione di percorsi accettabili per l'accesso esterno alle risorse facilita il monitoraggio. Limitando i protocolli non approvati e indirizzando le sessioni approvate a un percorso predefinito, le anomalie risultano più facili da individuare per eseguire ulteriori indagini, in cui strumenti SIEM e di logging possono aiutare a contrassegnare eventi anomali.

Best practice 4: evitare comandi non autorizzati ed errori

Diritti di accesso e autorizzazioni possono essere utilizzati per limitare l'accesso alle risorse IT. A volte, questo approccio non fornisce il livello di precisione necessario per controllare effettivamente le operazioni eseguite da un utente in un sistema. Ad esempio, un amministratore di sistema di terzi potrebbe dover accedere a un server mediante un account di tipo root o admin, un account super-utente con privilegi molto elevati. Questo approccio all'accesso, potenzialmente giustificato da motivazioni tecniche o amministrative, può però aprire la strada a una condizione di rischio. Quel livello di privilegio consente all'individuo di eseguire praticamente qualsiasi operazione all'interno del sistema, inclusa la sua cancellazione totale; un rischio inaccettabile per la maggioranza delle aziende, anche se il soggetto è un dipendente.

Un approccio diverso, che utilizza una soluzione di Privileged Access Management, offre un'alternativa più praticabile, consentendo un controllo delle autorizzazioni granulare per meglio gestire questo tipo di utenti. Un sistema di Privileged Access Management consente il brokering delle sessioni per conto di un utente su vari sistemi target utilizzando diversi account (ad esempio root), ognuno con livelli di autorizzazione specifici.

Anche filtraggio dei comandi, blacklist e whitelist possono essere utilizzati per limitare i comandi che uno specifico utente può eseguire. Una blacklist includerà i comandi non consentiti, mentre una whitelist i comandi che possono essere eseguiti; utilizzati insieme, forniscono un livello elevato di controllo e di flessibilità. In questo modo, l'utente con privilegi può gestire la risorsa senza causare danni inaccettabili. Un vantaggio secondario del filtraggio dei comandi è rappresentato dalla prevenzione degli errori involontari. Nell'esempio di cui sopra, il super utente sarà in grado di spostare i file, ma non di formattare il disco.

I filtri dei comandi, in combinazione con la registrazione, facilitano monitoraggio e avvisi: il sistema risponde in modo appropriato al tentativo di aggirare uno dei filtri, ad esempio generando un avviso o terminando una sessione sospetta. Ad esempio, un individuo potrebbe decidere di fare qualche esperimento prima di raggiungere i limiti imposti dai filtri dei comandi; quando i limiti vengono raggiunti, il sistema può generare un avviso che richiede di verificare le azioni di quell'utente. Tra le possibili risposte:

- Bloccare e avvisare l'utente
- Terminare la sessione
- Disabilitare l'account utente
- Generare avviso/allarme diretto al SOC

Best practice 5: monitorare e indagare

Un certo livello di monitoraggio è sempre necessario. Il livello e la portata specifici di questo monitoraggio dipendono però da considerazioni relative alla gestione del rischio e della compliance.

Anche in situazioni di rischio intrinseco minimo, la registrazione aiuta a risolvere i problemi e a indagare sulle attività sospette. La funzione di registrazione di base consiste nel documentare ciò che è avvenuto, pratica utile per rivedere attività inappropriate o non autorizzate. Questa registrazione include:

- Ora di accesso e disconnessione
- Sistemi oggetto di accesso
- Comandi eseguiti
- Risposte ricevute

In qualsiasi tipo di situazione delicata, il monitoraggio utilizza i log per applicare le policy definite per l'accesso al sistema, dato che i tentativi di violarle richiedono di intervenire. In risposta a un tentativo di violazione delle policy possono essere adottate diverse misure: a un livello di base, questi tentativi richiedono un'indagine per scoprire cosa è successo. Una formazione supplementare può essere richiesta per aiutare gli utenti a comprendere quali operazioni ci si aspetta da loro e come devono essere eseguite. Una violazione può essere il risultato di un semplice errore, oppure essere indicativa di un comportamento doloso. Il monitoraggio aiuta ad acquisire gli eventi sospetti, in modo che possano essere verificati.

Le indagini sono molto importanti, come illustrato dal caso di JPMorgan Chase, il cui personale ha scoperto di aver subito una violazione dopo aver svolto un'indagine su uno dei fornitori dell'azienda.

> "JPMorgan ha scoperto la presenza di hacker all'interno dei suoi sistemi nel mese di agosto, dopo aver inizialmente rilevato che lo stesso gruppo di hacker aveva violato il sito web di un evento di beneficenza sponsorizzata dalla banca... È stato solo dopo aver rilevato la violazione di questo sito che JPMorgan si è resa conto che la propria rete era stata attaccata dagli stessi hacker".
>
> "Neglected Server Provided Entry for JPMorgan Hackers"
> The New York Times, 22 dicembre 2014

In ambienti ancora più sensibili, la registrazione o l'acquisizione delle sessioni può essere necessaria per fornire informazioni complete su una determinata sessione, a supporto di indagini future. Un caso d'uso comune consiste nell'acquisire registrazioni a schermo intero di sessioni sensibili. Queste sessioni possono essere successivamente esaminate in caso di violazioni note delle policy o di problemi che si manifestino in un secondo tempo all'interno di un sistema, per valutare cos'è avvenuto nel corso della sessione originale. A seconda della sensibilità dell'ambiente, possono essere desiderabili anche controlli a campione. Una delle sfide tipicamente associate alla registrazione delle sessioni è rappresentata dal fatto che la registrazione di file (e il carico generale sul sistema) può costituire un'operazione imponente. L'altra sfida è costituita dalla necessità di un piano d'azione per riesaminare le sessioni registrate. Dal momento che sia la tecnologia che i costi, in base alla durata, aumentano per la registrazione delle sessioni, l'analisi costi-benefici aiuta a identificare le situazioni adeguate per questo livello di investimento. Come punto di partenza, è utile identificare quanto segue:

- Quando registrare e per quanto tempo
- Quando e con quale frequenza rivedere le registrazioni
- Qual è la policy di memorizzazione delle registrazioni

Se si sceglie di implementare tecniche di registrazione delle sessioni, emerge la rilevanza di varie funzionalità:

- Facile accesso ai metadati sulla sessione: quando è iniziata e quando si è conclusa
- Capacità di passare rapidamente da una sessione all'altra e a un punto specifico di una registrazione
- Capacità di evidenziare attività "degne di nota", come ad esempio violazioni delle policy e attività sensibili

Le situazioni a rischio più elevato possono giustificare un monitoraggio "over the shoulder" o l'accesso two party, in cui un secondo individuo controlla l'attività svolta da un utente con privilegi in tempo reale. In genere, queste situazioni di rischio estremo non si verificano con terzi o altri utenti esterni. Il monitoraggio di questo tipo presenta difficoltà di tipo tecnico. In aggiunta a esse, tuttavia, è necessario che chi monitora sia un soggetto altamente qualificato, in grado di comprendere le operazioni eseguite e le loro ramificazioni sull'ambiente più in generale. Da una prospettiva di gestione del rischio questo tipo di monitoraggio sarà adatto a un numero molto limitato di situazioni.

Il monitoraggio tipico include un processo in due fasi:

- **Risposta in tempo reale alle violazioni delle policy:** possono venire attivate varie azioni: invio di un avviso all'utente, generazione di un avviso inviato a un centro di Operations di sicurezza, blocco di una sessione o di un account.
- **Ricerche e analisi a posteriori:** una revisione dei log o delle registrazioni delle sessioni per supportare la risoluzione dei problemi o l'indagine forense.

La ricerca e l'analisi a posteriori possono includere attività per mettere in correlazione i log e gli avvisi generati da un sistema di Privileged Access Management con altri strumenti di rete e di sicurezza, in relazione a eventi anomali. Ad esempio, in un'azienda in cui è stata implementato una soluzione di Privileged Access Management, tutta l'attività amministrativa è centralizzata all'interno del sistema in questione. Se da altre parti della rete arrivano richieste di sessione SSH o Telnet, vengono viste come indicazioni immediate che qualcosa non va e verificate. Eliminando o vietando strumenti di amministrazione non autorizzati, le attività sospette risultano relativamente facili da identificare. Un firewall di nuova generazione è in grado di fornire supporto nell'evidenziare applicazioni o protocolli vietati. Altre attività sospette possono includere l'accesso in momenti imprevisti o comportamenti insoliti, come il download di file.

Nel corso del tempo, audit e verifiche manuali continui aiutano a mettere a punto strumenti e policy per ignorare i falsi positivi e automatizzare trigger e avvisi più efficaci.

Sezione 3

Vantaggi della gestione del rischio collegato ai terzi

Nessuna azienda moderna può essere isolata e non connessa a Internet. I rapporti di business richiedono modalità di collaborazione in forma elettronica in cui lo scambio di informazioni sensibili tra i partner è lo standard. Oggi, le aziende utilizzano fornitori terzi per servizi di contabilità, elaborazione delle carte di credito, consulenza legale, amministrazione dei piani pensionistici, servizi di marketing, produzione e centinaia di altri processi. La collaborazione elettronica tra partner di business consente di risparmiare tempo e denaro e rende possibili processi e sistemi automatizzati che migliorano la precisione, la qualità e l'efficienza. Limitare l'accesso di terzi alla rete a livello di firewall non è una soluzione. Le risorse rilevanti devono essere disponibili ai partner di business perché i vantaggi di business possano diventare realtà. Allo stesso tempo, il collegamento con terzi pone alle aziende rischi reali.

Le violazioni della sicurezza sono costose. Secondo la rivista Fortune, dopo il furto di 40 milioni di carte di pagamento e 70 milioni di altri dati alla fine del 2013, Target ha subito costi stimati per 162 milioni di dollari, già considerati i rimborsi percepiti dalle assicurazioni. Sony ha stimato esborsi per 35 milioni di dollari per "Ripristino di sistemi finanziari e IT" a seguito di una violazione subita nel 2014. Home Depot ha registrato 28 milioni di dollari di oneri netti al lordo delle imposte. E i costi citati non considerano i danni alla reputazione e l'aumento dei premi assicurativi. In aggiunta a questi costi "vivi", c'è l'effetto dirompente sulla vita delle persone coinvolte. Molti hanno perso il loro posto di lavoro, altri hanno dovuto lavorare giorno e notte per indagare e mitigare le violazioni.

> "A prescindere dal modo in cui la misuriamo o dal fatto che adottiamo un'ottica rivolta al futuro o al passato, concordiamo sul punto centrale che le aziende hanno bisogno di investire nella sicurezza delle informazioni".
>
> Benjamin Dean, ricercatore presso la School of International and Public Affairs della Columbia University, Fortune Magazine, 27 marzo 2015

Chiaramente, nessuna azienda vuole trovarsi in prima pagina sul Wall Street Journal ne ruolo di protagonista dell'ennesima violazione di rilievo. Le 5 best practice sulla sicurezza delle informazioni possono bloccare le violazioni, consentendo nel contempo le attività di business legittime, e mantenere così al sicuro risorse e reputazione dell'azienda.

Sezione 4

Conclusioni

Secondo il Data Breach Investigations Report (DBIR) 2015 di Verizon, 400 milioni di dollari di perdite finanziarie stimate sono stati il risultato di 700 milioni di documenti compromessi. Settanta aziende che hanno contribuito a questo report hanno documentato 79.790 incidenti di sicurezza, di cui 2.122 violazioni confermate in 61 paesi, con i due terzi degli incidenti verificatisi negli Stati Uniti. Anche se la maggior parte delle minacce provengono ancora da fonti esterne, le minacce interne e collegate ai partner sono aumentate leggermente tra il 2013 e il 2014. I rischi sono reali, come dimostra la rilevantissima violazione subita dall'Office of Personnel Management degli Stati Uniti.

Il metodo dell'attacco [a OPM] ha seguito una formula precisa: prendere di mira un subappaltatore mediante un attacco di social engineering e sottrarre le credenziali per ottenere l'accesso alla rete. Inserire un malware in un sistema e creare una backdoor. Estrarre i dati per mesi, all'insaputa dell'azienda.

La violazione ai danni di OPM ha evidenziato anche la vulnerabilità delle aziende alle azioni di social engineering. I dipendenti e gli appaltatori pubblici oggi devono seguire programmi di formazione di sensibilizzazione alla sicurezza per comprendere i pericoli dello spear phishing e di altre minacce social media.

> "The most innovative and damaging hacks of 2015"
>
> CSO Magazine, 28 dicembre 2015

Molti rischi possono essere attenuati adottando le cinque best practice descritte in questo documento, che operano in sinergia per attivare una difesa forte, flessibile e potente per proteggere le informazioni. Queste best practice includono:

- Implementare processi e controlli di supporto che definiscono e applicano policy per gli utenti di terze parti con privilegi.
- Migliorare l'autenticazione degli utenti mediante una tecnologia multi-fattore, affinché le credenziali con privilegi siano più difficili da violare, anche in caso di attacchi di social engineering e phishing.
- Separare l'autenticazione dal controllo degli accessi, per fare in modo che gli utenti con privilegi abbiano una visibilità limitata sulle reti interne, riducendo al minimo i danni che possono essere arrecati da un utente o dalla sottrazione di un singolo set di credenziali.
- Impedire comandi non autorizzati ed errori in modo che i trigger in tempo reale fungano da prima linea di difesa, proteggendo l'infrastruttura da tentativi dannosi ed errori involontari.
- Monitorare e indagare sulle attività sospette per individuare rapidamente le violazioni, migliorare la formazione quando necessario e perfezionare costantemente l'automazione e i processi per eliminare i falsi positivi.

I sistemi di Privileged Access Management includono funzioni e capacità automatizzate che consentono di definire, automatizzare e applicare le cinque best practice descritte in questo documento, nell'intera impresa, in ambienti fisici, virtuali e cloud, aiutando le aziende a implementare processi coerenti tra sistemi, device e applicazioni diversi.

Sezione 5

Riferimenti

https://www.brighttalk.com/webcast/9017/156931

http://www.xceedium.com/solutions/privileged-identity-management/432-2

http://www.bankinfosecurity.com/occ-more-third-party-risk-guidance-a-7233/op-1

http://www.bankinfosecurity.com/banks-vendor-monitoring-comes-up-short-a-8103

Report NYS Financial Services Department del 9 aprile, "Update on Cyber Security in the Banking Sector: Third Party Service Providers"
http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html?emc=edit_tu_20160301&nl=bits&nlid=59970007

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

http://www.cnbc.com/2015/07/22/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html

How Much do Data Breaches Cost Big Companies? Shockingly Little
http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/ March 27, 2015

http://fortune.com/tag/data-breach 2 marzo 2016

http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/10?itc=refresh 27 luglio 2015

https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx 21 agosto 2015

http://www.csoonline.com/article/3018343/security/the-most-innovative-and-damaging-hacks-of-2015.html

Sezione 6

L'autore

Dale R. Gardner vanta oltre due decenni di esperienza con il software enterprise, che vanno dalla gestione dei sistemi e delle reti a vari segmenti dell'ambito sicurezza, inclusi identity management, sicurezza delle applicazioni, gestione delle vulnerabilità, compliance e sicurezza della rete. Ex analista di ricerca e scrittore, ha definito, creato e commercializzato molteplici soluzioni per la gestione e la sicurezza che migliorano le Operations e contribuiscono a garantire l'integrità e l'affidabilità delle infrastrutture IT aziendali. Attualmente è responsabile del marketing globale del portfolio di prodotti di Privileged Access Management di CA Technologies.

Entra in contatto con CA Technologies 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 lavora 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_183401_0416