Documentazione tecnologica

McAfee
An Intel Company

PROTEZIONE DEI DATABASE

Migliorare la sicurezza contro gli attacchi e i vettori di perdita dei dati odierni

ARCHITETTURA DI RIFERIMENTO SECURITY CONNECTED

LIVELLO 1 2 **3** 4 5

Security Connected

La struttura Security Connected di McAfee permette l'integrazione di più prodotti, servizi e partnership per fornire una soluzione centralizzata, efficiente e efficace per la mitigazione del rischio. Basato su oltre vent'anni di pratiche di sicurezza comprovate, l'approccio Security Connected aiuta le aziende di qualsiasi dimensione e settore - in tutte le aree geografiche - a migliorare lo stato della sicurezza, ottimizzare la sicurezza per una maggior efficienza nei costi e allineare strategicamente la sicurezza con le iniziative di business. L'architettura di riferimento Security Connected fornisce un percorso concreto che va dalle idee all'implementazione. Utilizzalo per adattare i concetti Security Connected ai rischi, all'infrastruttura e agli obiettivi specifici della tua azienda. McAfee è impegnata senza sosta a ricercare nuovi modi per mantenere protetti i propri clienti.

Migliorare la sicurezza contro gli attacchi e i vettori di perdita dei dati odierni

La situazione

Nel 2010, la quantità di violazioni dei dati ha raggiunto il picco assoluto, e il 47% degli attacchi ha impiegato solo pochi minuti o ore per andare a segno e compromettere i sistemi. Un altro 44% ha impiegato qualche giorno, secondo il report 2011 Data Breach Investigations (Investigazioni sulle violazioni dei dati) di Verizon e dei Servizi Segreti degli Stati Uniti. I "cattivi" sono rapidi nell'andare a segno, mentre i "buoni" sono lenti a reagire. Il tempo intercorso tra un attacco e la sua scoperta è stato di settimane (38%) o mesi (36%)[1]: il che significa una gran quantità di tempo a disposizione dei criminali per ottenere ciò che vogliono e andarsene con eleganza.

I malintenzionati agiscono in minuti o giorni mentre i buoni reagiscono in settimane o mesi. Come fanno a muoversi così velocemente? Utilizzano nuove tattiche. Le principali tattiche utilizzate sono la pirateria informatica (50%) e il malware (49%). Inoltre, il report conclude che gli aggressori sono alla ricerca di "obiettivi leggeri", organizzazioni più piccole con pochi sistemi ben protetti, piuttosto che orientarsi verso aziende che dispongono di una folta schiera di server con milioni di record.

Spesso, gli aggressori ricevono un aiuto involontario dai dipendenti. Attraverso il social engineering e il furto di credenziali, gli aggressori possono trovare con facilità il modo di sembrare "personale interno" con accesso legittimo. E, dal momento che le risorse dei database sono preziose e il panorama economico è sconfortante, funziona anche la corruzione. Lo scorso anno, corruzione e tangenti sono state le tattiche sociali più utilizzate, secondo quanto afferma il report. Non ci si può perciò fidare del fatto che la protezione perimetrale mantenga il database al sicuro, né che i dipendenti facciano la cosa giusta.

Le principali preoccupazioni

I database non solo memorizzano informazioni critiche, ma spesso sono collegati a vari sistemi che forniscono servizi essenziali per l'azienda. Qualsiasi interruzione, divulgazione non intenzionale o perdita dei dati dai database ha il potenziale di mettere a repentaglio le operazioni e la reputazione di un'azienda. Inoltre, poiché un database conserva dati sensibili e regolamentati, una violazione a un database solitamente si traduce in una violazione di conformità, con costi di bonifica elevati, perdita di fiducia da parte dei consumatori e perdita drastica in termini di capitalizzazione del mercato.

Per proteggere i dati sensibili contro minacce esterne e interne, è necessaria una visibilità in tempo reale dell'attività del database. La maggior parte delle aziende odierne sfrutta gli strumenti di verifica e registrazione insiti nel database per proteggerlo, ma questi strumenti sono tristemente inadeguati contro le moderne tattiche di pirateria informatica e social engineering. Per proteggere in modo adeguato un database da codice dannoso e perdita di dati è necessario affrontare le seguenti preoccupazioni:

- **Monitoraggio di attività e cambiamenti**. Tutti i database rispondono ai comandi. Se il comando è appropriato per l'utente che richiede i dati, sarà efficace. Attacchi e strumenti diventano sempre più sofisticati consentendo agli aggressori di aggirare le tecniche di rilevamento tipiche e scalare i privilegi. Controlli dell'accesso mediocri facilitano il compito di un aggressore. Tipicamente, il livello di accesso assicurato agli utenti supera in modo significativo i diritti d'accesso di cui hanno bisogno sul sistema o richiedono per i loro ruoli. Account superati e controlli negligenti sulla creazione dei nuovi account mettono a disposizione degli aggressori un numero maggiore di possibili punti di ingresso. In primo luogo attaccano password inefficaci e predefinite e poi scalano i privilegi. Il monitoraggio delle attività sulla rete si è dimostrato un metodo inadeguato per questo problema, poiché i metodi di accesso locale possono aggirare i sistemi di monitoraggio basati sulla rete.

- **Strumenti di verifica**. Le funzionalità native di verifica e logging dei database non riescono a garantire la giusta visibilità. La maggior parte non individuerà le modifiche effettuate, i privilegi utilizzati, gli amministratori coinvolti o le modifiche a livello di sistema. Inoltre, le attività di logging e verifica integrate all'interno del database possono rallentare le prestazioni del database stesso. Gli amministratori possono anche disabilitare queste funzioni, progettate per il monitoraggio non per la sicurezza, eliminando qualsiasi valore che gli strumenti nativi possono aver fornito.
- **Patching senza interruzioni**. Profitti, tempo di attività e disponibilità hanno la meglio sulla sicurezza. Alcune aziende hanno un ciclo per l'applicazione delle patch ben superiore ai 12 mesi. Ci sono centinaia di nuove minacce ogni anno, ma a causa della natura critica dei database, le interruzioni non sono un'opzione. Le aziende desiderano essere costantemente protette senza dover aggiornare il database.
- **Supporto al cloud**. Le aziende iniziano a adottare il cloud e il database deve adattarsi per garantire accesso e monitoraggio utilizzando servizi cloud, non solo sulla rete locale.
- **Dimostrazione di conformità rispetto agli standard di settore, governativi e interni**. In base al ruolo del database, potrebbe essere necessario attenersi, creare report e mantenere policy per diverse normative, quali PCI DSS, Sarbanes-Oxley, HIPAA, SAS 70, GLBA e FERPA. E se si opera anche con altre nazioni, tenere presente che adottano requisiti similari per la privacy e il controllo finanziario. Inoltre, l'azienda potrebbe aver sviluppato best practice e standard operativi propri, e il management si aspetta dashboard che mostrino lo stato dei sistemi rispetto agli standard governativi.

Elementi decisionali
I seguenti fattori potrebbero influenzare l'architettura dell'azienda:

- Quali requisiti normativi deve seguire l'azienda?
- Come viene riportata e segnalata la conformità con le normative del database aziendale?
- L'azienda dispone di database che operano su sistemi operativi a 64-bit? Quali?
- Quale è il livello di sicurezza del database?
- Quanto spesso vengono aggiornati i database?

Descrizione della soluzione

Ogni azienda si affida a un database per operare. Se non ci si affida ai fornitori dei sistemi operativi per la protezione degli stessi, perché accontentarsi di strumenti forniti dal vendor per proteggere le risorse dei database più preziosi? I database presentano sfide uniche e tipicamente l'implementazione di policy e standard di sicurezza vengono lasciati nelle mani degli amministratori dei database. Le notizie sulle violazioni dei database riempiono le prime pagine dei giornali, perciò è necessario prendere in considerazione un nuovo approccio che possa garantire la protezione dell'integrità dei database contro codice dannoso e - triste ma vero - gli stessi dipendenti interni.

Per affrontare queste preoccupazioni, una soluzione deve essere in grado di soddisfare i seguenti requisiti:

- **Monitoraggio di attività e cambiamenti**. Una soluzione deve essere in grado di monitorare il comportamento e l'attività di tutti i database da un punto di osservazione esterno al database. Se quest'attività di monitoraggio venisse eseguita esclusivamente all'interno del database, gli amministratori dei database potrebbero disabilitare la funzione (volutamente o involontariamente). Inoltre, una soluzione deve anche essere in grado di chiudere una sessione che viola una policy, generare avvisi verso una console gestita centralmente e mettere in quarantena un utente dannoso o non conforme. Una soluzione deve essere in grado di rilevare le tecniche di aggiramento e evitare che vengano utilizzate.
- **Strumenti di verifica**. In modo analogo, gli strumenti di verifica sono inefficaci se un amministratore può disabilitarli. Una soluzione deve essere in grado di fornire funzionalità protette di verifica e logging esterne al database per garantire che i record vengano acquisiti e resi disponibili per l'analisi. Durante l'analisi forense post-incidente, questo processo di verifica può essere utile per identificare il volume dei dati persi e ottenere una maggiore visibilità sulle attività pericolose. Una soluzione deve essere in grado di fornire la registrazione di tutte le operazioni effettuate e report che soddisfino le normative SOX, PCI e altri requisiti per la verifica della conformità.
- **Patching senza interruzioni**. Una soluzione deve essere in grado di rilevare gli attacchi che cercano di sfruttare vulnerabilità note e i vettori delle minacce più comuni. Dovrebbe essere configurata in modo da inviare un avviso o chiudere la sessione in tempo reale. Aspettare che un fornitore di database renda disponibile una patch o evitare di applicare le patch per evitare cali di produttività rende i database vulnerabili a molti vettori di minaccia. Il concetto delle patch virtuali può aiutare a proteggersi contro le vulnerabilità nuove e zero-day e può essere implementato senza tempi di inattività del database, proteggendo i dati sensibili finché non è disponibile una patch da applicare.

- **Supporto al cloud**. Affidarsi all'analisi del traffico di rete per identificare le violazioni delle policy è un'operazione impossibile o inefficiente nelle architetture distribuite e altamente dinamiche utilizzate per la virtualizzazione dei data center e per il cloud computing. Una soluzione dovrebbe essere configurata per iniziare l'attività con ogni nuovo database, richiedere le policy di sicurezza basate sui dati ospitati, quindi inviare gli allarmi al server di gestione. Anche in caso di un'interruzione della connessione alla rete, i dati dovrebbero essere comunque protetti tramite policy applicate localmente.
- **Conformità rispetto agli standard di settore, governativi e interni**. Standard e normative cambiano, così come i report che si devono mantenere. Una soluzione deve fornire modelli normativi e per la conformità che vengono sostenuti con i controlli più recenti e assistenza alle violazioni. Una soluzione deve essere in grado di identificare le minacce nel momento in cui si verificano e creare report sulla prevenzione, riducendo rischio e responsabilità. I modelli preconfigurati dovrebbero includere le normative PCI-DSS, Sarbanes-Oxley, HIPAA e SAS-70, tutte visualizzabili da una piattaforma gestita centralmente.

Le tecnologie utilizzate dalla soluzione McAfee

McAfee offre due prodotti appositamente studiati per la sicurezza dei database, McAfee® Vulnerability Manager for Databases e McAfee Database Activity Monitoring. La gestione centralizzata tramite McAfee ePolicy Orchestrator® (McAfee ePO™) riunisce questi due prodotti in una piattaforma unificata per la gestione di sicurezza e conformità per l'intera infrastruttura.

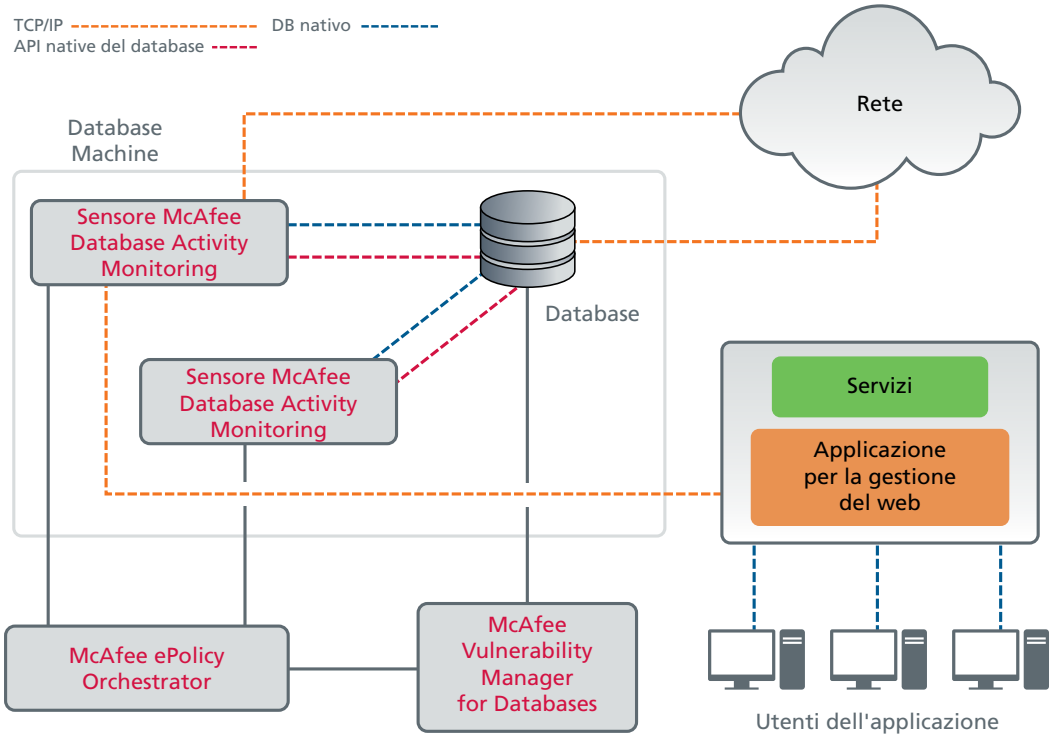
McAfee Vulnerability Manager for Databases esegue più di 3.000 controlli delle vulnerabilità sui principali sistemi di database come Server SQL, DB2, e MySQL. Migliorando la visibilità dei punti vulnerabili dei database - e fornendo le raccomandazioni degli esperti su come intervenire - McAfee Vulnerability Manager for Databases riduce le probabilità di una breccia pericolosa e fa risparmiare denaro tramite la migliore preparazione per le verifiche di conformità alle normative. McAfee Vulnerability Manager for Databases aiuta a ridurre la superficie d'attacco identificando i punti di debolezza tipici di cui sono alla ricerca aggressori e attacchi, quali password inefficaci, password condivise e account predefiniti. Per tracciare e rispondere a eventi sospetti, creando report relativi al livello di versione/patch, oggetti e privilegi modificati, e tracce scientifiche dagli strumenti comunemente utilizzati dagli hacker.

Diversamente dalle verifiche di base o dall'analisi dei log, che rivelano solo ciò che si è verificato dopo un evento, McAfee Database Activity Monitoring offe visibilità in tempo reale e funzioni di prevenzione delle intrusioni per chiudere le brecce prima che provochino danni. Oltre 380 regole predefinite risolvono problemi specifici mediante patch dei fornitori dei database, nonché profili di attacco generici. I modelli di policy pre-costruiti possono essere personalizzati per supportare le regole per l'accesso al database e processi appropriati e conformi.

Gli allarmi sono inviati direttamente alla dashboard di monitoraggio con i dettagli completi di qualsiasi violazione delle policy, allo scopo di eseguire gli interventi correttivi. In caso di violazioni ad alto rischio la configurazione può terminare automaticamente sessioni sospette e mettere in quarantena gli utenti malintenzionati, dando tempo al personale di sicurezza di investigare l'intrusione.

Gli attacchi che prendono di mira i preziosi dati memorizzati nei database possono provenire dalla rete, da utenti locali che accedono al server stesso e anche dall'interno del database, tramite procedure o attivatori memorizzati.

McAfee Database Activity Monitoring utilizza i sensori basati sulla memoria per monitorare l'attività e catturare tutti e tre i tipi di minacce con una singola soluzione non intrusiva. Gli aggiornamenti delle patch virtuali vengono forniti regolarmente per le nuove vulnerabilità scoperte e possono essere applicati senza il downtime del database, proteggendo i dati sensibili finché non viene rilasciata e applicata una patch del produttore del database. Le informazioni su attività e eventi possono quindi essere utilizzate per dimostrare la conformità a fini di verifica e migliorare la sicurezza nel suo complesso.



Protezioni specializzate permettono a McAfee di valutare le vulnerabilità del database e monitorare azioni dannose e pericolose.

McAfee Vulnerability Manager for Databases

Progettato per velocizzare le scansioni iniziali e i report predefiniti per rispondere alla maggior parte dei requisiti di conformità, McAfee Vulnerability Manager for Databases è in grado di individuare e analizzare diversi database da un'unica console. Localizza e identifica le tabelle contenenti informazioni sensibili e effettua una rapida scansione delle porte fornendo la versione e le patch applicate al database. Oltre alle funzioni di base per l'efficacia delle password (password semplici, predefinite e condivise), analizza le password hashed memorizzate, per esempio, con algoritmi SHA-1, MD5 o DES. Inoltre, identifica la suscettibilità ai rischi specifici dei database, fra i quali SQL injection, buffer overflow e codice PL/SQL malevolo o non protetto, presentando i risultati in report preconfigurati per gli standard di conformità più comuni.

McAfee Database Activity Monitoring

McAfee Database Activity Monitoring è un sensore di piccole dimensioni, un agent software che viene installato sul server del database e monitora l'intera attività. Il sensore è un processo standalone scritto utilizzando il linguaggio C++ che opera sul computer su cui risiede il database. Viene installato utilizzando strumenti con piattaforma standard (RPM, PKG, DEPOT, BFF, or EXE) in un account utente separato del sistema operativo sul computer. Il sensore identifica automaticamente tutte le istanze del database sul computer e può monitorare diverse istanze, anche diversi tipi di database, sullo stesso sistema.

Quando è in esecuzione, il sensore si associa all'area di memoria dell'istanza della cache SQL, utilizzando meccanismi di sola lettura e API (Application Programming Interface), e inizia il monitoraggio tramite un ciclo di polling di un campione di memoria. Per ogni ciclo, il sensore analizza le istruzioni in esecuzione e le precedenti per ogni sessione nell'istanza del database e, utilizzando una policy predefinita ricevuta dal server, stabilisce quali istruzioni dovrebbero essere segnalate o bloccate. Le istruzioni che violano la policy vengono inviate alla console di gestione in tempo reale come avvisi. Il sensore può anche essere configurato in modo da chiudere le sessioni in base a violazioni specifiche e mettere in quarantena gli utenti. Non è intrusivo e utilizza solo piccole quantità delle risorse della CPU (meno del 5% di un singolo core CPU, anche su computer multi-CPU). Le funzionalità di prevenzione del sensore vengono implementate utilizzando API native del database per consentirgli di chiudere le sessioni del database senza introdurre alcun rischio per l'integrità dei dati.

McAfee ePolicy Orchestrator (McAfee ePO)

McAfee ePO permette la distribuzione del sofware e la gestione delle policy in modo automatico e centralizzato. McAfee Vulnerability Manager for Databases è integrato nella dashboard McAfee ePO, fornendo così reportistica centralizzata e informazioni riepilogative su tutti i database. McAfee ePO si collega inoltre a McAfee Database Activity Monitoring per un'unica vista unificata e una reportistica ottimizzata.

L'impatto della soluzione

Introducendo una protezione specialistica per gli attacchi e i vettori di perdita dei dati dei database, viene migliorata la capacità di rilevare e respingere gli attacchi esterni, riducendo le possibilità di interruzione e rischio dall'interno della rete.

McAfee offre visibilità e protezione in tempo reale per tutte le fonti di attacco, monitorando e segnalando gli eventi sospetti. McAfee contribuisce a ridurre al minimo il rischio e la responsabilità bloccando gli attacchi prima che causino danni, sia che la minaccia arrivi dalla rete, dagli utenti locali collegati al server stesso o dall'interno del database. Il virtual patching di vulnerabilità del database di recente individuazione fornisce una protezione immediata senza tempi di inattività del database.

Modelli e regole predefinite, controlli automatici e aggiornati e interfacce basate su procedure guidate velocizzano la distribuzione e aiutano a ottenere un'architettura di sicurezza del database verificata in modo semplice e efficiente.

Risorse supplementari

www.mcafee.com/it/solutions/database-security/database-security.aspx
www.mcafee.com/it/products/vulnerability-manager-databases.aspx
www.mcafee.com/it/products/database-activity-monitoring.aspx
www.mcafee.com/it/products/epolicy-orchestrator.aspx

Per maggiori informazioni sull'architettura di riferimento Security Connected:
www.mcafee.com/it/enterprise/reference-architecture/index.aspx.

Informazioni sull'autore

Uy Huynh è senior director sales engineering di McAfee. Coordina il suo team in modo da fornire le soluzioni, le best practices e i progetti di sicurezza corretti per aiutare i clienti a migliorare lo stato della loro sicurezza e proteggere le risorse digitali più importanti. Uy è un esperto nel settore della sicurezza e ha collaborato con clienti Fortune 100 quali HP, Oracle, ATT, McKesson e altri, aiutandoli a scegliere i prodotti di sicurezza più adatti per soddisfare le loro complesse esigenze.

Prima di McAfee, ha creato e guidato l'organizzazione SE di Foundstone, presso cui ha sviluppato le best practice per la gestione di vulnerabilità e rischio per reti e sistemi di grandi dimensioni. Prima di Foundstone, è stato Senior Consultant di ISS dove ha sviluppato una gamma di soluzioni di sicurezza, policy e tecnologie per aziende di grandi dimensioni.

[1] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

38600bp_protecting-databases-L3_1111