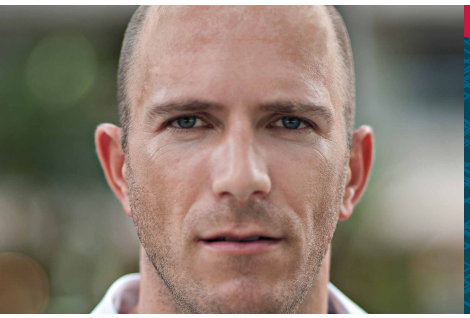

Cinque motivi per implementare una soluzione dedicata per la sicurezza del database

Instaurare un'ultima linea di difesa critica

Proteggere le informazioni preziose e riservate memorizzate all'interno dei database è fondamentale per mantenere l'integrità e la reputazione delle aziende in ogni luogo, per non citare la conformità con le normative. Tuttavia, molte aziende si affidano ancora a soluzioni di sicurezza con limiti intrinsechi. Date le complessità delle piattaforme database odierne e il livello di sofisticazione raggiunto oggi dai criminali informatici, la distribuzione di una soluzione completa e dedicata per la sicurezza del database è imprescindibile. Qui di seguito ecco cinque motivi che spiegano perché.

I benefici di McAfee Vulnerability Manager

- Piena visibilità sullo stato di sicurezza del database
- Analisi di molteplici database in tutta l'azienda da una console centralizzata
- Accelerazione del raggiungimento della conformità e riduzione dei cicli di verifica, con significativi risparmi sui costi
- Rapida distribuzione con una minima conoscenza del sistema database
- Rapida generazione di rapporti personalizzati in un formato di facile lettura per i diversi ruoli degli utenti

I benefici di McAfee Database Activity Monitoring

- Massima visibilità e protezione da tutte le fonti di attacco
- Monitoraggio delle minacce esterne, degli insider privilegiati e delle minacce sofisticate provenienti dall'interno del database
- Rischi e responsabilità ridotte fermando gli attacchi prima che provochino danni
- Risparmia tempo e denaro con un'implementazione più rapida e un'architettura più efficiente
- Flessibilità di un'installazione facile sull'infrastruttura IT scelta

1. Non puoi proteggere una risorsa se non sai che esiste

Anche negli ambienti IT aziendali più tradizionalisti, non è del tutto raro trovarvi centinaia o anche migliaia di istanze database contenenti informazioni estremamente sensibili. I dipartimenti IT verrebbero inoltre messi sotto pressione per fornire il numero esatto, l'ubicazione, il livello di sensibilità dei dati e lo stato di sicurezza di tali database. La parte peggiore è che i criminali lo sanno e sono sempre alla ricerca di lacune nella protezione. Dispongono del tempo e delle risorse tecniche necessarie per sfruttare quei database che ritenevi fossero al sicuro o di cui non conoscevi neanche l'esistenza. La tua mancanza di visibilità è per loro un'opportunità.

Puoi disporre di una visibilità completa del panorama dei database della tua azienda solo quando hai la possibilità di eseguire un accurato processo di discovery di tutti i database esistenti all'interno del tuo ambiente, unitamente a una scansione per identificare quali di questi contengono informazioni relative alle carte di pagamento, dati delle risorse umane, dati di vendita e altri dati sensibili. Inoltre, un test automatico approfondito delle vulnerabilità del database è fondamentale per stabilire l'esatta natura dei rischi. Solo una soluzione dedicata per la sicurezza dei database può fornirti informazioni dettagliate fruibili che possono prioritizzare e porre rimedio alle lacune nella sicurezza, permettendo all'azienda di risparmiare il costo, considerevole, di un consulente per la sicurezza esterno.

McAfee® Vulnerability Manager for Databases rileva automaticamente tutti i database presenti sulla rete, stabilisce se sono state applicate le patch più recenti ed effettua una scansione alla ricerca di vulnerabilità. McAfee Vulnerability Manager esegue oltre 4.200 controlli di vulnerabilità per i principali database e classifica le minacce in livelli di priorità distinti, fornendo script per risolvere i problemi e suggerimenti. Richiede una conoscenza minima dei database, genera report personalizzati in formati di facile comprensione per vari ruoli degli utenti e lo fa da una console di sicurezza centralizzata.

2. La sicurezza perimetrale non protegge contro le minacce interne

Hai investito una gran quantità di tempo, impegno e capitale nel selezionare e distribuire firewall e altre tecnologie per la sicurezza della rete. Tuttavia, come sai, non tutte le violazioni ai database hanno origine al di fuori del perimetro. Infatti, la ricerca annuale condotta dal Computer Emergency Response Team (CERT) indica che la metà delle violazioni dei database sono causate da utenti interni. Perciò, devi proteggere i tuoi dati aziendali più critici da avversari anche più insidiosi, vale a dire dipendenti con privilegi, molti dei quali hanno i mezzi per aggirare le funzionalità di sicurezza native di un sistema DBMS, manomettere i log d'accesso e nascondere le loro tracce.

La giusta soluzione per la sicurezza del database rileva e previene le minacce provenienti da tutti i possibili vettori: minacce che hanno origine dall'esterno e in particolare dall'interno. Inoltre, fornirà una struttura per impostare e applicare policy per l'accesso al database secondo requisiti specifici per la conformità per assicurare ininterrottamente una reale separazione delle mansioni.

McAfee Database Activity Monitoring rileva automaticamente i database in rete, li protegge con un insieme di difese preconfigurate, agevolando la creazione di una policy di sicurezza personalizzata per il proprio ambiente. Ciò rende più facile dimostrare la conformità ai revisori e migliorare la protezione delle risorse dati critiche. Con McAfee Database Activity Monitoring, hai visibilità sull'intera attività del database, compresi gli accessi con privilegi locali e gli attacchi sofisticati dall'interno del database. Protegge i dati da tutte le minacce monitorando localmente l'attività su ogni server database indipendentemente dall'ubicazione e inviando avvisi o terminando automaticamente le sessioni sospette o che violano in qualche modo la policy di sicurezza. McAfee Database Activity Monitoring protegge anche i database e applica le policy in ambienti virtualizzati o di cloud computing.

3. I malintenzionati possono attaccare più velocemente di quanto tu sia in grado di aggiornare i sistemi

Il martedì delle patch dovrebbe essere dichiarato un giorno di festa per gli hacker. Si tratta del giorno del mese in cui i produttori di database rivelano gli obiettivi più maturi. Inoltre, il martedì delle patch preallerta i malintenzionati perché sanno quanto sia faticoso per il gruppo che si occupa della gestione del database in azienda scollegare, aggiornare e testare i database. Infatti, contano proprio sul fatto che, poiché il processo di applicazione delle patch crea un notevole disagio operativo, sceglierai di ritardarlo il più a lungo possibile, dando loro tempo sufficiente per trovare un modo di intrufolarsi.

Non c'è modo per evitare il tradizionale processo di applicazione delle patch - e le vie d'accesso che offre ai criminali - a meno che non si disponga di una soluzione dedicata per la sicurezza dei database. E tale soluzione deve permettere di aggiornare lo stato della sicurezza dei database in tempo reale, senza affliggere lo staff e senza interrompere le attività aziendali.

McAfee Virtual Patching for Databases difende i database dal rischio associato alle vulnerabilità per le quali non sono stata ancora distribuite delle patch, individuando e prevenendo i tentativi di attacco e intrusione in tempo reale, senza richiedere la disattivazione del database o il test delle applicazioni. Ti permette di stare tranquillo, poiché hai la certezza di essere protetto dalle minacce anche durante i periodi di picco delle vulnerabilità, ovvero l'intervallo temporale che intercorre tra il rilascio delle patch da parte dei vendor e l'effettiva installazione delle stesse.

McAfee Database Activity Monitoring è un'altra soluzione non intrusiva che offre un livello aggiuntivo di protezione durante il martedì delle patch e oltre. I suoi sensori di memoria intercettano gli attacchi che prendono di mira i database che provengono dalla rete, da utenti locali che accedono al server stesso e anche dall'interno del database, tramite procedure o attivatori memorizzati.

4. Non è possibile continuare a sacrificare la conformità a favore della continuità

I requisiti per la conformità con le normative applicabili in settori come la sanità, la finanza e la vendita al dettaglio sono in costante evoluzione e diventano sempre più rigorosi in corso d'opera. Non sorprende che i database più critici per l'azienda vengano pesantemente influenzati dalle pratiche per la conformità, che impongono che i database vengano aggiornati con le patch più recenti fornite dai produttori di sistemi DBMS. Tuttavia, data la natura onerosa del processo per scollegare, aggiornare e quindi testare più database di diverse tipologie, la maggior parte delle aziende sacrifica la conformità per preservare la business continuity. Inoltre, potrebbero esserci database legacy ancora in uso per cui non sono nemmeno disponibili degli aggiornamenti per le vulnerabilità.

Con McAfee Virtual Patching for Databases, puoi mantenere la business continuity senza sacrificare la conformità con le normative. Permette di pianificare come preferisci le tradizionali attività di applicazione delle patch, sapendo che i database sono sicuri e conformi. McAfee Virtual Patching for Databases è una soluzione che permette di risparmiare molto tempo, oltre che un valido controllo di compensazione agli occhi dei revisori della conformità. Inoltre, permette anche di estendere la protezione più recente ai database legacy che non sono più supportati dai produttori di sistemi DBMS.

I benefici di McAfee Virtual Patching for Databases

- Protezione dalle minacce ancora prima di installare gli aggiornamenti di patch resi disponibili dai fornitori
- Nessuna necessità per i gruppi dedicati alla sicurezza e all'IT di avere conoscenze specifiche relative ai sistemi DBMS
- Grazie alla struttura non intrusiva del software, è possibile mantenere online i database di produzione
- Protezione costante dei database grazie alla distribuzione automatica degli aggiornamenti
- Conformità semplificata con standard quali PCI DSS, HIPAA e altri

I benefici del software McAfee ePolicy Orchestrator

- Visibilità completa della protezione del database e della conformità da una console di gestione centralizzata
- Un punto di vista unico permette di riunire facilmente i database in un programma di gestione della sicurezza unificato, on premise, presso uffici remoti e anche nel cloud
- Un'architettura aperta e flessibile che collega la gestione delle soluzioni di sicurezza McAfee e di terze parti ai tuoi strumenti di gestione LDAP, operazioni IT e configurazione

5. Quando i dati risiedono nel cloud, la visibilità è estremamente limitata

Il cloud offre incredibili vantaggi operativi e risparmio dei costi IT ma, come è risaputo, c'è un problema: il tuo staff può perdere il controllo dei dati sensibili e non disporre di alcuna visibilità su chi vi potrebbe accedere. Tuttavia, implementando la soluzione giusta per la sicurezza del database puoi proteggere i tuoi dati negli ambienti fisici e virtuali. La giusta soluzione può prevenire attività non autorizzate del database e può segnalare le attività alla tua console di gestione, anche in caso il database sia virtualizzato o risieda nel cloud.

Grazie alla sua implementazione unica di sensori di memoria, McAfee Database Activity Monitoring può essere configurato per essere fornito automaticamente a ogni nuova macchina virtuale. Allo stesso tempo, può richiedere policy di sicurezza sulla base dei dati che ospita e quindi iniziare a inviare avvisi al server di gestione. Inoltre, i suoi sensori possono operare autonomamente anche quando scollegati dal server, in modo che i dati sensibili siano protetti e preservati indipendentemente dal fatto che il database sia online o meno o dove sia ubicato in qualsiasi momento. Anche se la connettività di rete viene interrotta, i dati restano protetti dato che il sensore applica le policy di sicurezza a livello locale, e gli allarmi sono messi in coda per essere consegnati quando il server di gestione torna raggiungibile.

Inoltre, l'accesso ai database nel cloud può essere monitorato tramite il software McAfee® ePolicy Orchestrator® (McAfee ePO™), una console per la gestione della sicurezza aziendale per una visibilità completa della sicurezza del database e dell'azienda e della conformità.

In altre parole, cloud o non cloud, tu e il tuo staff potete godere dei più elevati livelli di visibilità. Chiaramente, McAfee offre la soluzione per la sicurezza del database più adatta per il tuo ambiente IT, indipendentemente dalle dimensioni della tua attività e quanto siano sensibili i tuoi dati.

I benefici offerti dalle soluzioni per la sicurezza del database di McAfee

- Facilità di distribuzione e utilizzo
- Piena visibilità sullo stato di sicurezza del database
- Allineamento delle pratiche di amministrazione delle policy di sicurezza tra il personale preposto alla sicurezza e alla gestione del database
- Conformità con le normative costante e efficiente
- Rischi e responsabilità ridotte fermando gli attacchi prima che provochino danni
- Gestione della sicurezza del database da una console centralizzata

Scopri maggiori dettagli su come mantenere i tuoi database protetti e disponibili

McAfee è consapevole del fatto che i database aziendali conservano la maggior parte delle risorse critiche dell'impresa. Devono essere disponibili ventiquatt'ore al giorno per supportare l'attività dell'azienda. E, così come i tuoi database non vanno mai in vacanza, anche noi siamo sempre attivi. Ecco perché affermiamo che la sicurezza non dorme mai. Ti assicuriamo che il nostro team di esperti di sicurezza del database è concentrato senza sosta a mantenere le informazioni sensibili al sicuro e disponibili, aiutando la tua azienda a assicurare la conformità con le policy interne e le normative di settore.

Per informazioni più dettagliate su come le soluzioni McAfee per la sicurezza del database possono aiutarti a proteggere i database business-critical, visita il sito www.mcafee.com/it/products/database-security/index.aspx o contatta il tuo rappresentante McAfee o rivenditore locale.

Seguici su Twitter: @McAfee_DBSecure.

A proposito delle soluzioni McAfee per la protezione degli endpoint

McAfee, società interamente controllata da Intel Corporation (NASDAQ:INTC), è la principale azienda focalizzata sulle tecnologie di sicurezza. Le nostre soluzioni di nuova generazione per la protezione degli endpoint offrono protezione per tutti i dispositivi, oltre ai dati e alle applicazioni che contengono. Queste soluzioni, complete e personalizzate, riducono la complessità per raggiungere una protezione multilivello degli endpoint, senza mettere a rischio la produttività. Offrono il mix perfetto tra analisi tradizionale del malware, whitelisting dinamico, prevenzione delle intrusioni comportamentali zero-day, gestione unificata e intelligence sulle minacce integrata. Maggiori informazioni su www.mcafee.com/it/products/endpoint-protection/index.aspx.

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

41903brf_top5-db-sec_0212_fnl_ASD