



McAfee
An Intel Company

PROTEZIONE DEL DATA CENTER

Guida alla soluzione

Epsilon: dopo la violazione

Nel 2011, una violazione dei dati di Epsilon, società specializzata in marketing via e-mail, ha portato alla diffusione dei nomi e degli indirizzi e-mail di milioni di clienti. Dato che un gran numero di aziende molto note si avvale dei servizi di Epsilon, ne è scaturita un'ondata di notifiche ai clienti delle stesse, relativamente a potenziali frodi. Tra le aziende che hanno dovuto avvisare la propria clientela erano comprese: Barclaycard US, Capital One, Best Buy, JPMorgan, Citigroup, TiVo, Disney Destinations, New York & Company, Walgreens, Marriott e molte altre. (Fonte: <http://mcaf.ee/5342e>)

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 McAfee 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.

Una sicurezza maggiore per un data center più agile

Le sfide

I data center permettono alle aziende di operare. Tra i ruoli di un data center vi è la generazione di fatturato, la conservazione di dati sensibili e la fornitura di servizi business-critical. Data la loro criticità e valore, diventano degli obiettivi. Dati sensibili, applicazioni di business, database, dispositivi di rete, storage e infrastruttura di supporto sono tutti da tempo nel mirino di aggressori esterni e interni nonché di revisori armati di mandati normativi.

Praticamente ogni problema legato alla sicurezza dei data center e mandato normativo ha generato una soluzione singola non integrata. Questo processo reattivo, dove nuove soluzioni singole non integrate vengono aggiunte ogni volta, ha portato a controlli del data center che sono complessi, numerosi, costosi e incoerenti, opprimendo così la maggior parte delle aziende. Oltre ai requisiti esistenti, nuove minacce e tendenze entrano costantemente nella mischia. Per esempio, le aziende richiedono che i data center supportino la mobilità e il Web 2.0 fornendo protezione contro attacchi mirati e opportunistici, e che il tutto venga fatto riducendo al minimo i tempi di fermo e producendo report frequenti per dimostrare la conformità.

La tradizionale protezione per i data center manca di quelle caratteristiche di business agility necessarie per adottare i nuovi requisiti in modo rapido e senza problemi, delle funzioni di gestione della sicurezza necessarie per essere efficienti ed efficaci, della disponibilità e dell'integrità necessaria per le operazioni mission-critical odierne e del design ottimizzato per l'efficienza dei costi. I data center hanno assunto un ruolo più fondamentale che mai. I dipartimenti IT odierni stanno aprendo nuove vie. Possiamo solo fare speculazioni su quale sarà la "grande idea rivoluzionaria" tra cinque anni, ma se utilizziamo gli ultimi cinque anni come metro di misura, ciò che pensavamo ci rendesse sicuri non ci manterrà protetti. È necessaria una struttura strategica che aiuti a riunire e collegare questi pezzi storicamente eterogenei.

In base al report di marzo 2011 del Ponemon Institute "Cost of a Data Breach" (Il costo di una violazione dei dati), ogni record compromesso costa 214 dollari, raggiungendo una media di 7,2 milioni di dollari per ogni violazione dei dati².

Heartland Payment Systems dopo la violazione

Nel 2010 Heartland ha concluso una conciliazione da 60 milioni di dollari con VISA per soddisfare le richieste di risarcimento collegate alla violazione del 2009. Un anno prima, Heartland aveva raggiunto un accordo simile con Amex per 3,5 milioni di dollari¹.



Soluzioni

Business agility

Al gruppo operativo del data center sono state assegnate responsabilità che vanno dalla creazione di soluzioni per garantire conformità e virtualizzazione costanti al consolidamento e allo sfruttamento del cloud. Una struttura di sicurezza dovrebbe essere sufficientemente snella e agile per consentire un rapido cambiamento e l'adozione di nuovi trend senza aggiungere altri rischi. Una solida struttura di sicurezza che consente di avere questo livello di agilità ha un impatto positivo sulle operazioni aziendali e di sicurezza.

Gestione della sicurezza

Le violazioni sono costose, con costi che vanno da sanzioni normative, azioni di classe e costi per le pubbliche relazioni fino a quelli legati a una minor fedeltà al marchio, clienti persi e, in ultima analisi, minori guadagni. Data la complessità dei data center unitamente ai suddetti trend e minacce, un'azione riuscita di mitigazione del rischio richiede un approccio olistico alla sicurezza. Dovrebbe essere utilizzata una soluzione per la gestione centralizzata della sicurezza che collega diverse soluzioni per dati, endpoint, reti e cloud quando si gestiscono data center di ogni dimensione e complessità. Una gestione flessibile della sicurezza è fondamentale per avere visibilità su applicazioni e database che elaborano le transazioni e i dispositivi di storage che conservano quei dati.

Disponibilità e integrità

Fornire disponibilità e integrità a fronte di minacce interne e esterne è una sfida complessa, ma anche adottare nuovi trend come gli equivalenti mobili dei siti web, integrare servizi Web 2.0 di terze parti o sfruttare le varie infrastrutture cloud. E può anche essere estremamente rischioso se non si adotta un certo livello di attenzione nel fornire un solido stato di sicurezza che non sia focalizzato in modo miope sulla sicurezza dei contenuti o della rete ma piuttosto miscela sicurezza di endpoint, contenuti e rete integrandosi con il cloud. Una struttura di sicurezza dovrebbe ridurre al minimo i tempi di latenza, diminuire il rischio rappresentato da errori di configurazione manuale, vietare l'installazione

di software pericoloso e proteggere le informazioni a prescindere dalla tipologia del data center, che sia consolidato, virtualizzato o basato su cloud. La protezione degli ambienti virtualizzati - server virtualizzati e infrastrutture VDI (Virtualized Desktop Infrastructure) - è fondamentale. Un'infrastruttura VDI è comunemente installata su qualsiasi dispositivo, dagli smartphone ai laptop ai server virtuali, e questa rappresenta la norma nei data center. Le soluzioni odierne devono essere ottimizzate in modo da poter affrontare i trend in ambito virtualizzazione, ma anche i principi base sono importanti. Tempi di latenza e tempi di fermo non programmati non sono accettabili in ambienti mission-critical. Operazioni di rete, controllo degli accessi, protezione degli endpoint e firewall devono tutti essere progettati tenendo ben presente le esigenze dei dipartimenti IT operativi: non solo sicurezza, poiché soluzioni di sicurezza sotto la media che introducono tempi di latenza possono essere dannosi tanto quanto un attacco.

Ottimizzazione della sicurezza

L'ottimizzazione della sicurezza sposta le aziende dalla questione puramente tecnica relativamente ai controlli di sicurezza - "Possiamo farlo?" - per affrontare la seguente domanda: "Quale è il modo migliore per farlo?". Esistono molte soluzioni di sicurezza e la maggior parte svolgono un buon lavoro. Ma complessivamente introducono il fattore della complessità, il maggior nemico della sicurezza. Una situazione in cui sono presenti diversi sistemi isolati e soluzioni che non si collegano l'uno all'altro e dipendono da risorse sempre maggiori per funzionare non è sostenibile. Piuttosto, le strutture di sicurezza attuali dovrebbero supportare un modello di protezione ottimizzato volto a gestire centralmente i controlli di sicurezza, consentire l'integrazione tra i diversi controlli e allineare le soluzioni con le priorità di business riducendo i costi operativi per la sicurezza. Le minacce evolvono e una quantità maggiore di nuovi trend vengono adottati con rapidità: una struttura di sicurezza ottimizzata diventerà imprescindibile per attività aziendali efficienti, sicure e convenienti. Le soluzioni ottimizzate sono una parte integrante dell'automazione del processo di conformità in modo che attività e processi di sicurezza relativi ai mandati normativi siano allineati senza dar luogo a un ulteriore impiego di risorse.

Considerazioni sulle best practice

- Comprendere che i data center stanno attraverso una fase di rapido cambiamento: consolidamento, virtualizzazione e cloud
- Implementare soluzione che soddisfano le esigenze in termini di: agilità, gestione della sicurezza, disponibilità e integrità e ottimizzazione della sicurezza
- Implementare soluzioni che centralizzano le operazioni di sicurezza per i principali componenti del data center: reti, soluzioni virtualizzate, database, server e dispositivi di storage
- Garantire che le soluzioni di sicurezza utilizzate offrano supporto anche nel processo di automazione della conformità
- Quando ci si dedica alla sicurezza, assicurarsi che i principi operativi relativi a disponibilità e latenza vengano presi in considerazione

Secondo la Data Loss DB Open Security Foundation, dell'aprile 2011, il 75% degli episodi di perdita dei dati è stata una conseguenza di un'attività nefasta mentre la restante percentuale è attribuita a disattenzione³.

Requisiti di valore

I progetti per il data center della tua azienda dovrebbero sfruttare tecnologia basata sulla sicurezza per stimolare l'efficienza operativa. È necessario prendere in considerazione le seguenti aree in cui è possibile ottimizzare i data center:

- **Consolidamento** - Le soluzioni per il consolidamento dovrebbero essere implementate su hardware, software e infrastruttura di supporto.
- **Standardizzazione** - Le soluzioni dovrebbero supportare la standardizzazione delle funzionalità di protezione di endpoint, dati e rete. Ciò aiuterà ad assicurare che l'analisi delle minacce e le risposte relative siano efficaci.
- **Riduzione dei costi di verifica, conformità e monitoraggio** - Le soluzioni dovrebbero consentire (o essere giustificate da) una riduzione dei costi per la verifica IT e la conformità, dal momento che è possibile verificare i sistemi e il processo invece che tutti i nodi individuali.
- **Riduzione del traffico di rete** - Le soluzioni che sono presenti al cuore fungono da protezione e dovrebbero anche contribuire a eliminare traffico di rete inutile e spam.
- **Riduzione dei costi di help desk** - Le attività per proteggere il data center dovrebbero portare a una riduzione delle chiamate da parte dell'utente finale all'help desk per incidenti relativi alla sicurezza.

Materiali correlati dall'architettura di riferimento McAfee Security Connected

Livello II

- Protezione delle informazioni
- Controllo e monitoraggio del cambiamento

Livello III

- Valutazione delle vulnerabilità
- Applicare la conformità agli endpoint
- Prevenire gli attacchi Denial of Service (DoS e DDoS)
- Protezione dei server

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

Informazioni sull'autore



Brian Contos, professionista certificato per la sicurezza dei sistemi informatici (CISSP), è direttore della strategia globale per la sicurezza di McAfee. È un esperto di sicurezza riconosciuto con un'esperienza quasi ventennale nella progettazione e gestione della sicurezza. È autore di vari libri, tra cui *Enemy at the Water Cooler* (Il nemico al distributore dell'acqua) e *Physical and Logical Security Convergence* (Convergenza tra sicurezza fisica e logica). Ha collaborato con organizzazioni governative e aziende della classifica Forbes Global 2000 in America del Nord, del Sud e Centrale, Europa, Medio Oriente e Asia. Viene invitato come oratore a importanti eventi industriali quali RSA, Interop, SANS, OWASP e SecTor e collabora con la stampa di settore e economica come *Forbes*, *New York Times* e *The Times of London*. Brian è Distinguished Fellow del Ponemon Institute e laureato all'Università dell'Arizona.

brian_contos@mcafee.com || <http://siblog.mcafee.com/author/brian-contos/> || @BrianContos

¹ <http://mcaf.ee/gvxkh>

² <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf>

³ <http://datalossdb.org/>

