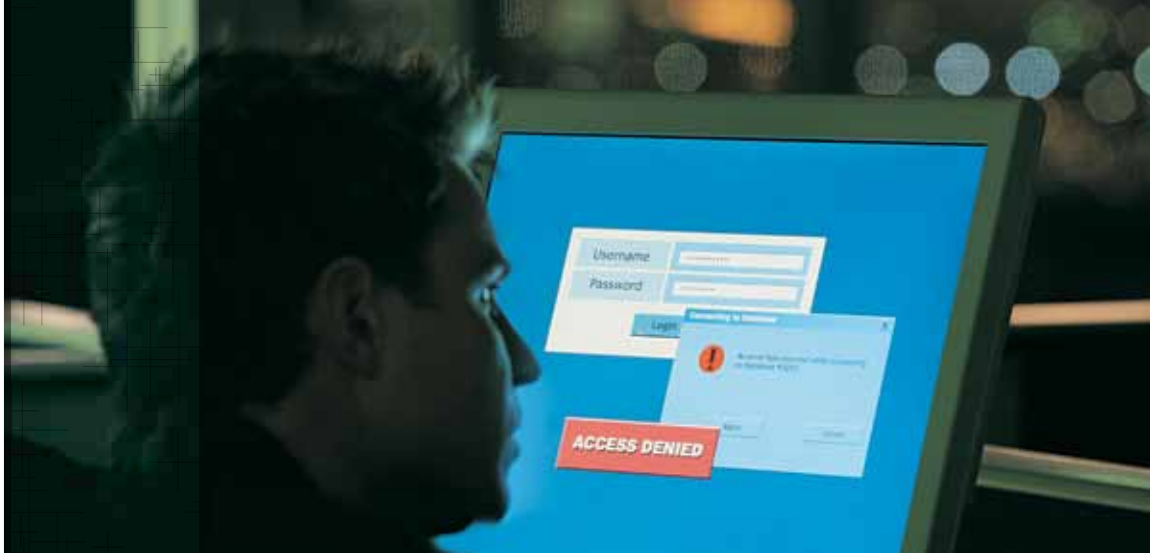
McAfee
An Intel Company

GESTIONE DI SICUREZZA E RISCHIO

Guida alla soluzione



Security Connected

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

Scaricate le più recenti risorse da www.mcafee.com/it/enterprise/reference-architecture/index.aspx.

Un approccio proattivo alla gestione del rischio

Le sfide

Conformità e rischio finanziario in passato rappresentavano le principali preoccupazioni per la gestione della sicurezza e del rischio. Gli audit e i processi di governance erano eventi prevedibili che il reparto IT tentava di semplificare e automatizzare. Il rischio era pertanto un concetto piuttosto statico. Tuttavia, l'attuale ritmo delle minacce (sia quelle a basso profilo e lente, come gli attacchi mirati, sia quelle fulminee come gli attacchi dei cyber-attivisti e i contagi malware) richiede che i dirigenti e gli amministratori IT prestino maggiore attenzione agli eventi in evoluzione e prendano decisioni rapide incentrate al rischio per la mitigazione.

Naturalmente, anche la conformità e il rischio finanziario sono diventati fattori dinamici. Si consideri che le autorità di regolamentazione approntano in modo indipendente più di 200 linee guida in tutto il mondo mentre l'impennata economica rimodella le opportunità di business. Lo scenario del rischio, che una volta era statico, adesso è mutevole come un caleidoscopio.

Analisi di grandi quantità di dati sulla sicurezza

La gestione del rischio oggi significa gestire una quantità maggiore di dati: scansioni delle vulnerabilità, registri di applicazioni e database, flussi, record di accessi e sessioni, avvisi e analisi delle tendenze. I flussi di dati provengono da diversi sistemi che proteggono diversi utenti con diversi dispositivi in diversi luoghi.

Gli audit, a prescindere che siano attivati internamente o esternamente, portano alla luce le difficoltà dovute alla gestione di dati provenienti da questa varietà di fonti. Gli amministratori IT devono rintracciare e raccogliere i flussi di dati nel formato preferito dal revisore per l'accesso. Gli audit sono per definizione una valutazione a ritroso e statica del rischio trascorso, che sottrae risorse organizzative e rallenta la gestione proattiva del rischio, la capacità di guardare avanti, di comprendere e mitigare i rischi in evoluzione prima che possano causare danni.

Valutazione del rischio

Il mondo odierno è un ambiente "Big Data", contenente enormi quantità di dati di sicurezza. La valutazione delle minacce alla sicurezza più sofisticate può richiedere giorni o mesi. La maggior parte degli analisti di sicurezza si trova ad affrontare problematiche di gestione dei dati paragonabili a quelle che riguardano gli amministratori IT che devono affrontare un audit: La mole di di flussi di dati indipendenti rende difficile formare un quadro sintetico e coerente degli eventi. Più grande è la massa di dati che vengono raccolti e analizzati, più sembrerà caotica e più tempo ci vorrà per ricostruire gli eventi. Solo quando il quadro sarà completo, quindi molto tempo dopo il verificarsi dell'evento, sarà possibile adeguare le policy e le protezioni per evitare che il problema si ripresenti.

E se l'attacco è fulmineo e dirompente, come un denial-of-service o un worm in rapida diffusione? Tempi di analisi di giorni o mesi per diagnosticare il problema potrebbero provocare un impatto gravissimo e potenzialmente fatale a livello di conformità ed esposizione finanziaria. Quali risorse sono realmente esposte al rischio della minaccia e quali sono dotate di controlli compensativi o di contromisure? Per rispondere a questa domanda, gli amministratori devono disporre di visibilità sullo stato di sicurezza dell'intera gamma dei loro sistemi, compresa la molteplicità in continua espansione di dispositivi mobili e personali che accedono alle loro reti.

Azioni mirate agli eventi

Dopo la comprensione si passa alla cernita e alla remediation. Quali sono le risorse che contano di più? Quali invece possono attendere? Gli amministratori spesso si dividono tra diverse console di gestione per eseguire scansioni, eseguire script, adeguare le policy, installare aggiornamenti o mettere sistemi in quarantena. Ogni prodotto che viene proposto sul mercato della sicurezza aggiunge costi e complessità: nuova interfaccia utente, nuovo formato dei dati, nuovo standard sulle policy, o nuovi report. Inevitabilmente, vi sono delle lacune di copertura e degli errori che espongono l'organizzazione e le sue risorse a rischi inutili e spesso non riconosciuti.

Non potete più permettervi osservare il rischio dallo specchietto retrovisore. Dovete guardare avanti, con una lente grandangolare che permetta di identificare e gestire il rischio man mano che si evolve. Le informazioni sulle situazioni a rischio consentono di accedere al contesto dinamico sull'ambiente globale delle minacce, sulle risorse e sulla situazione di sicurezza della propria azienda. Le tecnologie automatizzate per la gestione del rischio utilizzano questo contesto per aiutarvi costantemente ad analizzare le situazioni e mettere a punto policy e protezioni.

Soluzioni

Le grandi moli di dati di sicurezza e le inerenti questioni operative complicano la gestione della sicurezza e del rischio, ma una strategia globale abbinata alla tecnologia moderna può contribuire a rendere comprensibile il caos. Nell'ambito dei processi di gestione della conformità e dei rischi finanziari, è necessario prendere in considerazione, in tempo reale, i possibili rischi introdotti da eventi esterni ed interni. L'unificazione di questi sforzi permette di semplificare i processi e supportare risposte automatiche che tagliano i costi e i tempi di risposta. I dirigenti ottengono una maggiore visibilità sul potenziale impatto degli eventi di sicurezza sull'esposizione al rischio, mentre gli amministratori ottengono le informazioni dettagliate e il controllo necessari per mitigare il rischio in modo proattivo.

I moderni sistemi di gestione eventi di sicurezza e informativi (SIEM) funzionano a stretto contatto con la gestione della sicurezza e della conformità di dispositivi, server, reti, applicazioni e database. Questa piattaforma di gestione della sicurezza è in grado di fornire un nucleo di comando e controllo che facilita la visibilità e l'agilità operativa. Più questi sistemi si integrano reciprocamente, con la risk intelligence e con i sistemi di sicurezza, tanto più facilmente l'amministratore sarà in grado di comprendere e gestire i rischi. Un approccio basato sulle piattaforme permette di allineare e unificare i processi, le politiche, i flussi di lavoro e i report che normalmente sono individuali e frammentati. L'integrazione di informazioni strategiche aggiornate permette di inserire i dati nel contesto del rischio mutevole e contribuisce a migliorare l'accuratezza, la pertinenza e i tempi di risposta per ridurre il rischio.

Valutazione delle vulnerabilità

Le entità più regolamentate eseguono la scansione delle vulnerabilità a sostegno dei mandati di conformità. Tuttavia, le scansioni pianificate non raggiungono regolarmente i sistemi remoti e in ibernazione o non analizzano le attività business-critical come le applicazioni e i database. I sistemi inaffidabili potrebbero passare inosservati e ospitare vulnerabilità sfruttabili. Un approccio consapevole alla gestione delle vulnerabilità attraverso risorse di rete è in grado tenere conto di queste moltitudini di sistemi e di eliminare le lacune nella conformità. È possibile utilizzare l'intelligenza dinamica dei rischi, il valore delle risorse e le contromisure corrispondenti per l'esecuzione delle scansioni o l'applicazione di controlli compensativi.

Miglioramento della comprensione delle situazioni

A fronte di attacchi informatici e di perimetri permeabili, la maggior parte delle organizzazioni desidera comprendere e rispondere meglio ai rischi mutevoli. La chiave sta nel trovare i dati che contano, mentre ancora contano. Essendo dotati della velocità e della capacità di gestire le moli di dati di sicurezza, gli strumenti SIEM sono in grado di monitorare le applicazioni e i database, gestire i registri e normalizzare gli eventi in dashboard correlate. Alcuni di essi offrono inoltre informazioni in tempo reale sul panorama delle minacce, degli utenti, dei sistemi, dei dati, dei rischi e delle contromisure. Grazie a questo ricco quadro contestuale, è possibile capire rapidamente le attività legate alla sicurezza, comprese quelle trascorse. Gli strumenti di analisi più solidi consentono di prevedere e individuare gli attacchi e di risolvere le minacce nel giro di pochi minuti anziché di giorni.

Analisi approfondita del traffico di rete

Le reti costituiscono sia infrastrutture critiche sia condotti da cui possono fuoriuscire dati sensibili e regolamentati. Attraverso il monitoraggio e la gestione del traffico di rete, compreso il traffico crittografato, gli amministratori possono ridurre i rischi indesiderati o rischiosi di Internet e delle applicazioni e garantire l'applicazione delle policy sui contenuti. L'integrazione dei sistemi di sicurezza di rete della prossima generazione con SIEM e con le soluzioni di sicurezza per sistemi può aiutare i manager del rischio ad applicare le policy, difendersi dalle minacce zero-day e monitorare, analizzare e creare report sulla conformità.

Gestione ottimizzata dei registri

I registri rappresentano un patrimonio di dati a supporto della e-discovery, degli audit e di altri requisiti di conformità, a patto di sapere assorbire e selezionare i flussi di dati per potere individuare gli eventi rilevanti. Utilizzando una soluzione di gestione registri integrata, sicura e ad alte prestazioni, è possibile raccogliere i dati in tempo reale da tutte le fonti rilevanti e conservare i registri in base a uno standard sicuro sulla catena di custodia dei dati. Il controllo applicazioni è in grado di garantire che gli autori di attacchi non siano in grado di assumere il controllo dei sistemi di registrazione per nascondere le loro azioni. Il collegamento delle funzioni di gestione registri ad altre funzioni di sicurezza e di analisi del rischio consente di fare pervenire i dati di registro a chi può utilizzarli in modo ottimale per gestire il rischio.

Considerazioni sulle best practice

- Allineare e unificare processi e controlli frammentati
- Automatizzare le operazioni di raccolta, correlazione, valutazione, risposta e monitoraggio
- Sfruttare le informazioni dinamiche sul rischio, l'analisi degli scenari e la risposta basata su policy per identificare e bloccare le minacce
- Assicurare che i programmi relativi a rischi e protezione coprano tutti i dispositivi, i dati e l'infrastruttura informatica
- Riunire in una singola piattaforma tutte le informazioni relative a rischi e protezione provenienti dall'azienda, consentendo una gestione più efficiente ed efficace
- Monitorare la situazione costantemente e in modo proattivo per rilevare e rispondere al rischio in evoluzione, rispettare la conformità e prevenire gli eventi di sicurezza futuri

I processi manuali di protezione e prevenzione dei rischi hanno maggiori probabilità di inefficacia e contribuiscono ad aumentare i costi legati a sicurezza e conformità.

Offrire vantaggi concreti

Una strategia completa di gestione della sicurezza e del rischio agevolata da una piattaforma di gestione consapevole dei rischi e automatizzata aiuterà la vostra organizzazione a:

- Ottenere una significativa consapevolezza della situazione attraverso contesto e analisi ricchi di informazioni
- Diagnosticare e reagire agli incidenti entro pochi secondi anziché ore, per ridurre i danni, prevenire le violazioni dei dati e ridurre i costi della remediation
- Esporsi a un numero inferiore di eventi di sicurezza e conformità e ridurre i costi di ogni evento
- Semplificare i processi delle policy di conformità e di reporting per migliorare l'efficienza operativa
- Ridurre il numero di piattaforme, hardware e software utilizzati per la gestione della sicurezza
- Ridurre i tempi di formazione e i costi operativi

Materiali correlati dall'architettura di riferimento Security Connected

Livello II

- Controllo e monitoraggio del cambiamento
- Protezione del centro dati
- Vantaggi ottenibili dallo standard PCI

Livello III

- Valutazione delle vulnerabilità
- Miglioramento della comprensione delle situazioni
- Analisi approfondita del traffico di rete
- Gestione ottimizzata dei registri
- Indagini sulle violazioni dei dati
- Coabitazione con i social media
- Protezione della proprietà intellettuale

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

Informazioni sull'autore

Barbara G. Kay, CISSP (Certified Information Systems Security Professional), è un'analista di settore presso il Secure By Design Group. È specializzata nella protezione delle informazioni per le imprese distribuite e mobili e nell'educazione dei consumatori sull'uso sicuro di Internet. Prima di fondare Secure By Design nel 2006, Barbara ha coperto la carica di direttore del marketing per la Security and Privacy Initiative di Sun. Ha ottenuto la laurea presso il Dartmouth College.

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