Wüstenrot Gruppe

Profilo cliente
- Grande azienda austriaca fornitrice di servizi finanziari operante nel settore edile ed assicurativo

Settore
- Servizi finanziari

Ambiente IT
- 3.500 dipendenti

Problema
- La precedente soluzione SIEM non supportava in modo efficiente le esigenze in continua evoluzione dell'azienda

La soluzione McAfee
- McAfee Enterprise Security Manager

Risultati
- Implementazione in soli 15 giorni
- Prestazioni elevate, registrazione accurata dei dati da 100 origini diverse
- Gestione di oltre 1.000 eventi al minuto
- Solide capacità di archiviazione e cifratura dei registri
- Dashboard configurabili per supportare una gamma completa di tipi di dati e di rapporti

McAfee ESM aumenta la visibilità sulla sicurezza di banche e compagnie di assicurazione

Con i suoi oltre 3.500 dipendenti e 3,5 milioni di clienti, Wüstenrot Gruppe è una delle aziende fornitrici di servizi finanziari più importanti d'Austria. L'azienda è organizzata in due divisioni: una società che opera nel settore edile e offre prestiti bancari e mutui per progetti di costruzione residenziale e il gruppo Wüstenrot Insurance. Wüstenrot ha filiali in Repubblica Ceca, Slovacchia, Ungheria, Slovenia e Croazia.

Sfida aziendale: garantire la sicurezza delle operazioni bancarie e assicurative

Dati e sicurezza di rete sono fattori critici per il successo di qualsiasi azienda attiva nel settore bancario e assicurativo. Per salvaguardare la propria reputazione e la fiducia dei suoi clienti, Wüstenrot mira a mantenere i più alti livelli di protezione, soprattutto per quanto riguarda i dati sensibili dei clienti e la gestione delle reti e dei sistemi bancari.

In precedenza, per l'elaborazione e l'analisi dei registri degli eventi di sicurezza Wüstenrot utilizzava IBM Tivoli Compliance Insight Manager, soluzione che si è tuttavia rivelata inadeguata alle continue esigenze di evoluzione e di crescita dell'azienda. Wüstenrot ha quindi stabilito numerosi requisiti per scegliere una nuova soluzione SIEM (Security Information and Event Management, gestione delle informazioni e degli eventi di sicurezza). La richiesta era una soluzione chiavi in mano completa che includesse hardware e sistema operativo con una semplice funzione di reportistica, raccolta registri senza agent e supporto per metriche di monitoraggio come BASILEA II, PCI DSS e ISO 27002. Inoltre, Wüstenrot desiderava una soluzione che garantisse l'immediata disponibilità di tutti gli eventi verificatisi negli ultimi cinque giorni e la registrazione dei dati provenienti da Oracle HPUX, Windows Server, Microsoft SQL Server, CheckPoint e McAfee ePolicy Orchestrator (ePO). Wüstenrot cercava un fornitore SIEM che non ponesse limitazioni alla licenza relativamente al numero di origini dei registri e che garantisse buoni costi di manutenzione.

Perché McAfee: SIEM ad alte prestazioni

In base a tali requisiti, McAfee Enterprise Security Manager (ESM) è subito diventata la scelta privilegiata per Wüstenrot, ma l'azienda ha comunque preferito eseguire un test sulla soluzione SIEM con un'implementazione proof-of-concept (PoC) prima di prendere una decisione definitiva. In modalità PoC, McAfee ESM doveva registrare dati da ogni origine nel proprio ambiente e poi verificare che gli output e le prestazioni corrispondessero alle specifiche interne di Wüstenrot. Gli integratori di sistemi Auriga Systems e COMGUARD sono riusciti a implementare McAfee ESM in meno di un giorno, durante il quale si è tenuto anche un breve seminario sulle funzionalità avanzate di questa soluzione e sulla reciproca approvazione delle metriche per una riuscita perfetta del PoC. Dopo una prova di un mese, McAfee ESM ha ampiamente dimostrato la capacità di collegarsi a tutte le origini dei registri richieste.

La soluzione McAfee

Considerato il successo del PoC e la convenienza dei prezzi applicati da McAfee, Wüstenrot ha infine scelto la soluzione McAfee ESM ETM-4600-ELM. Grazie alla sua capacità di registrare almeno 1.000 eventi al secondo (EPS), McAfee ESM era la soluzione ideale per Wüstenrot.

Lavorando a stretto contatto con gli integratori di sistemi, il reparto IT di Wüstenrot è riuscito a implementare McAfee ESM in appena 15 giorni. La possibilità di collegarsi a 100 diverse origini dei registri ha consentito di registrare ottime prestazioni e un elevatissimo grado di precisione a livello di analisi dei registri.

"McAfee Enterprise Security Manager è una soluzione snella ed efficiente che ci permette di gestire eventi relativi a diversi mesi in pochi secondi e di ottenere immediatamente informazioni significative. Le dashboard sono molto intuitive e sono sempre a disposizione mia e del nostro team addetto alla sicurezza. Così possiamo individuare facilmente i problemi e reagire in tempi rapidi."

— Bc. Jiří Dolejš,
responsabile della sicurezza,
Wüstenrot

Una volta eseguita l'implementazione completa delle origini dei registri, il team addetto all'implementazione ha configurato le dashboard e i rapporti in base alle specifiche preconcordate in varie aree chiave. Tali specifiche riguardavano, tra le altre cose, modifiche dei livelli di autorizzazione per Active Directory, interruzioni e riavvii di server, eventi antivirus all'interno dell'infrastruttura e nuovi dispositivi rilevati sulla rete.

L'assistenza tecnica di McAfee ha prontamente fornito una soluzione efficace per risolvere l'unico problema verificatosi durante l'implementazione, vale a dire un formato data/ora non compatibile per il registro di verifica del database Oracle. McAfee ha messo a punto un formato data/ora speciale all'interno dell'ambiente nativo Oracle.

Piani futuri

McAfee ESM supera di gran lunga il requisito iniziale fissato da Wüstenrot, che richiedeva la disponibilità immediata degli eventi verificatisi negli ultimi cinque giorni, perché consente l'elaborazione tempestiva delle informazioni di registro aggregate per un periodo fino a un anno.

La prima fase di implementazione ha riguardato il lancio della soluzione SIEM e l'inserimento dei dati; ora Wüstenrot sta lavorando per aggiungere dashboard analitiche per aree selezionate da mettere a disposizione del reparto sicurezza. Inoltre, sta perfezionando le regole di correlazione per eliminare i falsi positivi delle regole predefinite.

L'archiviazione dei registri nella forma originale può prevedere limitazioni solo a causa della mancanza di spazio. Wüstenrot ha stabilito standard elevati per quanto riguarda l'integrità e la riservatezza dei registri archiviati e ha quindi predisposto hardware con array di archiviazione dedicati per i registri che sfruttano funzioni di crittografia certificate in McAfee ELM. Wüstenrot si è data come primo obiettivo l'archiviazione dei registri di un anno e sta attualmente curando la preparazione degli array di archiviazione. Il prossimo passo sarà l'attivazione della funzione di archiviazione registri con indicizzazione per la ricerca full-text tramite McAfee Enterprise Log Manager.

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

61188cs_wustenrot_0614