CASE STUDY

"Dopo attente analisi abbiamo scelto SGBox quale partner ideale che avrebbe potuto facilmente integrarsi con i nostri sistemi. Si è rivelata essere una piattaforma di log aperta in grado di raccogliere le informazioni proveniente da qualsiasi tipologia di sistema. È di facile utilizzo e rapida implementazione ed è compatibile con tutte le infrastrutture di sicurezza IT"

Fabrizio Di Narda
IT Security Infrastructure
EMEA Electrolux

Overview

Electrolux è un leader globale nel settore degli elettrodomestici e delle apparecchiature per uso professionale. L'azienda vende ogni anno più di 50 milioni di prodotti ai consumatori di più di 150 Paesi e offre soluzioni innovative sviluppate sulla base di approfondite ricerche sul consumatore per incontrare i desideri dei consumatori e dei professionisti di oggi. I prodotti di Electrolux includono frigoriferi, lavastoviglie, lavatrici, elettrodomestici da cucina, condizionatori e piccoli elettrodomestici come aspirapolveri, tutti venduti con marchi come Electrolux, AEG, Zanussi e Frigidaire.
Nel 2014, Electrolux ha raggiunto un fatturato di circa 12 miliardi di euro con un totale di 60.000 dipendenti.
Electrolux vanta in Italia importanti unità produttive e circa 6.000 dipendenti. Opera attraverso società industriali, distributive e di servizio sia nel settore degli elettrodomestici, per gestire l'offerta rivolta al mercato delle famiglie, che in quello delle apparecchiature professionali, per servire l'utenza professionale.
Electrolux Italia Spa produce circa 3,8 milioni di elettrodomestici all'anno nelle sue quattro fabbriche e svolge inoltre un ruolo importante nell'innovazione attraverso i suoi laboratori di Ricerca & Sviluppo, Progettazione e il suo Data Center.

Challenge

Tutti i componenti che costituiscono l'infrastruttura di sicurezza ICT di Electrolux generano una grande quantità di log eterogenei. Log che sono informazioni importanti e devono essere conservati e convertiti in un singolo formato che può essere gestito centralmente. Se si verifica una violazione dei dati sull'infrastruttura di rete, i log storici devono essere facilmente accessibili e dovrebbero essere in grado di essere correlati per aiutare l'amministratore di sistema a monitorare le informazioni specifiche.
Electrolux aveva la necessità di possedere un sistema per la gestione centralizzata dei log che gli permettesse di rafforzare la sicurezza di tutta l'infrastruttura IT. Dal momento che nella maggior parte dei casi, ogni sistema produce un formato proprietario di log, in caso di violazione dei dati tutti i record storici non avrebbero potuto essere salvati o accessibili facilmente per trovare e risolvere il problema. Questo avrebbe portato ad un ritardo nell'infrastruttura IT con perdita di tempo e denaro.

AZIENDA
Electrolux

SETTORE
Manifatturiero

IMPLEMENTAZIONE
Log Management

OBIETTIVI
- *Incrementare la sicurezza IT*
- *Ricerche rapide e precise*
- *Gestione dinamica delle informazioni raccolte*

LA SODDISFAZIONE DEL CLIENTE È IL NOSTRO OBIETTIVO

> *Un sistema di gestione dei log è obbligatorio per tutti i componenti critici dell'infrastruttura di sicurezza ICT al fine di ridurre i rischi derivanti dalla perdita dei dati*

Fabrizio Di Narda
IT Security Infrastructure EMEA
Electrolux

Soluzione adottata

Electrolux ha adottato la soluzione di SGBox implementando il modulo SG-Log che consente di raccogliere i log di qualsiasi formato proveniente da qualsiasi fonte di dati. I log raccolti, conservati in formato cifrato e originale, sono processati per estrarre gli eventi associati che possono essere facilmente analizzati in tempo reale o su base storica.

In questo modo è possibile raggiungere un accesso ottimale di normalizzazione, e raccogliere e riconoscere eventi significativi della rete, come, ad esempio, errori rilevati su alcune richieste da parte di load balancer e proxy inverso. Inoltre, consente di rilevare anomalie sul numero di attacchi ricevuti dalla rete, sia internamente che esternamente.

Proprio come le aziende, anche la rete produce un gran numero di log eterogenei, ciascuno nel proprio formato proprietario. SGBox è in grado di gestire in modo nativo standard syslog ma è anche progettata per raccogliere log di tutte le dimensioni. Electrolux, dopo aver implementato il modulo di SGBox, ha deciso quanti gruppi logici dividono l'infrastruttura monitorata. Sono stati creati due distinti gruppi: uno per raccogliere informazioni fornite da servizi UNIX e un altro per i load balancer.

I dati raccolti in questo modo sono pronti ed utilizzabili per tutte le funzioni di analisi che sono disponibili nativamente sulla piattaforma. La soluzione SGBox è utilizzata per la gestione dei log, in esecuzione su hardware e log aperti in fase di ricezione per alcuni dispositivi come BlueCoat Proxy e Check Point Firewall e attualmente per la gestione degli eventi per più di 70 dispositivi.

Sviluppi futuri

SGBox è risultata essere una soluzione altamente efficace per le finalità dell'azienda. Con il suo utilizzo, Electrolux è riuscita ad ottenere un sistema centralizzato per la gestione di tutte le informazioni e i log provenienti da tutta la rete aziendale. Questo ha permesso di incrementare la sicurezza dei lavoratori, rafforzata ulteriormente dalla capacità di SGBox di predire eventi pericolosi ancora prima che accadano, con la conseguente ottimizzazione dei tempi e dei costi di ogni risoluzione dei problemi. Electrolux ha in programma in futuro di estendere l'utilizzo di SGBox.

L'azienda prevede di sfruttare l'utilizzo di log del server in termini di correlazione di eventi e di utilizzo del modulo di monitoraggio della rete che è stato sviluppato per estendere la soluzione a tutti i dispositivi di rete.