CASE STUDY

> *SGBox ha un potente motore di riconoscimento e normalizzazione dei log che, attraverso un'interfaccia semplice e intuitiva, ci permette di aggregare log originati dai sistemi aziendali. I dati così raccolti vengono analizzati sia in tempo reale che su base storica. Apprezziamo particolarmente la possibilità di creare dashboard personalizzate, per una più immediata visualizzazione dei report*

Tiziano Malaguti
IT Manager del Comune di Modena

Overview

Tutte le realtà aziendali, comprese quelle della pubblica amministrazione, non possono sottrarsi agli adempimenti di legge in materia di protezione dei dati e privacy. Infatti, la sicurezza informatica è una priorità anche per le realtà locali come i comuni ed è per questo che il municipio di Modena ha scelto di affidarsi alle soluzioni d SGBox per rispondere alle necessità di sicurezza della propria infrastruttura informatica. Modena è un comune italiano di circa 185.045 abitanti, capoluogo dell'omonima provincia in Emilia-Romagna. La città di Modena è stata fondata nel 183 a.C., come colonia di diritto romano. Dal 1589 al 1859 fu capitale del Ducato di Modena e Reggio ed è un'antica sede universitaria ed arcivescovile. Il Palazzo Ducale fu sede già nel 1859 della Scuola militare dell'Italia centrale del Regno di Sardegna, evolutasi nei decenni fino a divenire nel 1947 Accademia Militare dell'Esercito e dell'Arma dei Carabinieri. Il Duomo, la Torre Civica e la Piazza Grande della città sono inseriti, dal 1997, nella lista dei siti italiani patrimonio dell'umanità dall'UNESCO.

Challenge

Il comune del capoluogo emiliano aveva la necessità di gestire in modo efficace, sicuro e centralizzato i log generati dal proprio sistema informatico, consentendo il monitoraggio puntale di una serie di attività come gli accessi effettuati in un dato lasso temporale (evidenziando anche quelli avvenuti fuori dall'orario di lavoro, quelli non andati a buon fine o quelli tramite VPN) , le transazioni fallite, eventuali anomalie (sia software che hardware) , possibili minacce malware. L'obiettivo chiaramente posto dall'amministrazione pubblica è stato quello di avere a disposizione un tool potente, ma facile da usare, che garantisse il massimo livello di protezione anche in termini preventivi. La soluzione richiesta a SGBox doveva essere in grado di gestire log in formato proprietario, consentendo analisi dinamiche e sistemi di anti-manipolazione. Non solo ma il Comune di Modena ha chiesto anche di poter intercettare gli incidenti e le anomalie; analizzare il comportamento degli utenti; migliorare le funzionalità di investigazione; gestire configurazione e vulnerabilità.

AZIENDA
Comune di Modena

SETTORE
Pubblica Amministrazione

IMPLEMENTAZIONE
Log Management e Correlation

OBIETTIVI
- *Gestione dei log*
- *Integrazione con applicativi eterogenei*
- *Compliance al D.Lgs. 196*

LA SODDISFAZIONE DEL CLIENTE È IL NOSTRO OBIETTIVO

> *"Grazie anche alla possibilità di definire e utilizzare KPI complessi, la piattaforma di SGBox risulta uno strumento indispensabile in grado di rilevare anomalie anche inusuali rispetto ad un traffico di dati apparentemente omogeneo"*

Tiziano Malaguti
IT Manager del Comune di Modena

Soluzione adottata

Il comune emiliano ha implementato la soluzione di SGBox per ottenere un sistema di monitoraggio potente e versatile su tutti i propri sistemi aziendali.
L'unica piattaforma sul mercato capace di rispondere in modo puntuale a tutti questi elementi è quella di SGBox, grazie alla possibilità di analizzare log provenienti da qualunque fonte di dati e di offrire un'analisi personalizzata sia in tempo reale, sia su base storica.
Attraverso il motore di correlazione, Il Comune di Modena ha potuto creare regole per individuare relazioni tra due o più log (catene di eventi) da una fonte dati singola o da più sorgenti, basandosi su valori preesistenti come il timestamp, l'indirizzo IP, il tipo di evento, ma anche aggiungendo nuovi parametri come la geolocalizzazione, la risoluzione dei nomi a dominio e la creazione di alias.

SGBox ha permesso di definire e utilizzare KPI complessi in grado di rilevare anomalie anche inusuali rispetto ad un traffico di dati apparentemente omogeneo. Proprio questa capacità è una caratteristica fondamentale per la rilevazione di frodi, intrusioni nella rete e altri eventi significativi che sarebbero impossibili da identificare.

A proposito di SGBox

Dalla competenza pluriennale nel settore dell'ICT Security come fornitore di soluzioni e servizi ad alto valore aggiunto nasce SGBox che offre una soluzione per la correlazione di eventi e analisi dei log per ottenere un controllo capillare della rete aziendale. La piattaforma SGBox è una soluzione SIEM modulare per la gestione dei log, il vulnerability management, il rilevamento di attacchi informatici, la conformità e l'auditing che, grazie alla sua architettura scalabile, si adatta alle imprese di tutte le dimensioni. La sua architettura modulare e distribuita consente di adattarne l'utilizzo alle differenti esigenze aziendali. Con SGBox è possibile generare viste aggregate con le informazioni raccolte dai vari moduli. Le informazioni collezionate alimentano inoltre un motore di correlazione in grado di generare allarmi e contromisure automatiche a fronte di attacchi o incidenti informatici.