

CASE STUDY

“
ODCEC necessitava di una piattaforma come SGBox in grado di raccogliere log da qualsiasi fonte dati effettuando analisi in tempo reale sulle informazioni raccolte per rilevare e rispondere alle minacce informatiche, indirizzare problematiche di Compliance o semplicemente effettuare attività di auditing automatiche
”

Giuseppe De Dominicis
Responsabile Ufficio Sistemi Informativi ODCEC – Roma

AZIENDA

Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma

SETTORE

Ordine Professionale

IMPLEMENTAZIONE

Log Management, Correlation, System Monitoring e Vulnerability Scanner

OBIETTIVI

- Piattaforma unificata per la conformità ai requisiti del GDPR (General Data Protection Regulation)



Overview

L'Ordine dei Dottori Commercialisti e degli Esperti Contabili (ODCEC) è nato nel 2008 dalla fusione dell'Ordine dei Dottori Commercialisti e l'Ordine dei Ragionieri Commercialisti e Periti Commerciali, ed è articolato in vari enti pubblici non economici a carattere associativo, ovvero il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili e gli Ordini Territoriali.

L'Ordine svolge le sue funzioni e persegue le sue finalità istituzionali attraverso il Consiglio, composto da 15 membri, e nominato dall'Assemblea degli iscritti in carica quattro anni, ad eccezione del primo mandato che ha durata quinquennale. Il mandato è rinnovabile per non più di due volte consecutive. La tenuta dell'Albo rappresenta una delle funzioni di autogoverno degli ordini professionali in oggetto. Ciascun Ordine territoriale cura la tenuta dell'Albo, verificando i requisiti di iscrizione e le cause di incompatibilità, e provvede alle iscrizioni e cancellazioni previste dalla legge professionale. Per lo svolgimento di tale funzione il Consiglio dell'Ordine si avvale dell'ausilio di un'apposita Commissione. L'Albo a sua volta è suddiviso in due distinte Sezioni, la A "Commercialisti" e la B "Esperti Contabili" cui corrispondono le relative suddivisioni dei tirocinanti e due ulteriori gruppi speciali, dedicati ai professionisti comunitari che esercitano la professione nel nostro Paese in modo temporaneo ed occasionale (articoli 9-15 del D. Lgs. 206/2007) ed una alle Società tra Professionisti (L. 183/2011 - D. Lgs. 34/ 2013).

Challenge

La priorità di ODCEC era prima di tutto quella di essere in linea con le richieste del Regolamento Europeo per la protezione dei dati. In secondo luogo, c'era l'esigenza di aumentare la sicurezza dell'infrastruttura IT con avvisi automatici e in tempo reale in caso di situazioni anomale o eventuali data breach.

LA SODDISFAZIONE DEL CLIENTE È IL NOSTRO OBIETTIVO

“

SGBox è ideale sia per monitorare la sicurezza informatica interna ed esterna, oltre che conservare i log degli amministratori di rete. L'implementazione nella sua totalità della soluzione SGBox ha permesso l'adeguamento alla normativa GDPR

”

Giuseppe De Dominicis
Responsabile Ufficio Sistemi
Informativi ODCEC – Roma

Soluzione adottata

ODCEC Roma ha adottato e integrato all'interno dei propri sistemi la totalità dei moduli di cui è composta la soluzione SGBox: Log Management (LM), System Monitoring (SM), Vulnerability Scanner (NVS) e Log Correlation Engine (LCE).

Nello specifico, il modulo Log Management è utilizzato per centralizzare log provenienti dal Firewall, per la registrazione degli accessi VPN e per l'autenticazione alla console di amministrazione. Mediante l'utilizzo dell'agent proprietario di SGBox è stato possibile registrare eventi dai server Windows.

Il modulo di Log Management ha permesso ad ODCEC di essere conforme alla normativa prevista dal D. Lgs. 196 che impone di registrare e conservare in maniera immutata i log di accesso degli amministratori di sistema.

Il modulo System Monitoring controlla l'intera infrastruttura di rete di ODCEC e individua possibili problemi prima che si verifichino effettuando un monitoraggio continuato dei server e degli

apparati di rete.

L'adozione del modulo Vulnerability Scanner permette di controllare il network, gestendo tutte le informazioni raccolte e gli allarmi generati in modalità aggregata e di effettuare scansioni sugli asset rilevando la presenza di vulnerabilità che saranno quindi eliminate per abbassare il rischio di attacco e il conseguente rischio di compromissione del dato.

Attraverso il modulo di Log Correlation, il cuore di SGBox, che genera allarmi e contromisure automatiche, sono state create specifiche regole di correlazione tra due e più log (catene di eventi) generati dai moduli LM, SM e NVS. Nello specifico sono state create regole per l'individuazione di cancellazione file e cartelle sul file server, cambi di password e modifica Audit Policy Windows.

L'adozione della soluzione SGBox da parte di ODCEC ha garantito il raggiungimento della compliance GDPR.



A proposito di SGBox

SGBox è un security vendor dinamico e innovativo con oltre 10 anni di esperienza nella produzione di software. In forte espansione nei mercati europei e mediorientali. SGBox ridefinisce l'approccio alla cyber security e compliance (GDPR, SAMA, ISO27001, PCI-DSS, ...) proponendo una soluzione integrata ma modulare, scalabile e di facile utilizzo in grado di adattarsi alle crescenti richieste del mercato. SGBox è disponibile "on-premise" e in cloud nella versione multitenant dedicata ai partner MSSP.