SGBOX

GENERAL DATA PROTECTION REGULATION

SGBOX E CONFORMITÀ CON IL GDPR

SGBOX
E CONFORMITÀ CON IL GDPR

Regolamento UE 679/2016

L'entrata in vigore del regolamento UE 679/2016 (General Data Protection Regulation o GDPR), che impone alle organizzazioni di tutelare i dati personali dei cittadini comunitari, ha avuto sin dall'inizio un impatto immediato sui sistemi informativi.
È stato in particolare il principio di accountability (2 comma, art. 5) a imporre al titolare del trattamento l'obbligo di dimostrare l'effettivo rispetto della normativa, valutando l'adeguatezza delle soluzioni tecnologiche adottate e la relativa efficacia nella tutela dei dati personali. La violazione del regolamento può determinare (da parte dell'autorità di controllo, articolo 58) responsabilità amministrative (la cui entità è descritta nell'articolo 83) e penali (articoli 167, 168, 169).
In questo contesto, uno dei principali strumenti di prova per il tracciamento delle attività di gestione dei dati è il log generato dai dispositivi informatici.

Le piattaforme di Security information and event management (SIEM) hanno improvvisamente acquistato un peso rilevante, anche in considerazione della possibilità di raccogliere in modo organizzato le informazioni riguardanti gli accessi.
SGBox è una piattaforma next generation SIEM modulare per la gestione intelligente dei dati proposta in modalità cloud, appliance virtuale o fisica. Ogni modulo, attivabile individualmente, ha una sua specifica funzionalità e coopera con gli altri moduli per condividere le informazioni raccolte, facilitando la conformità con i requisiti imposti dal GDPR.

Il GDPR chiede implicitamente di definire una data-destruction policy (retention period) rispettando il principio del diritto all'oblio del data subject (interessato). SGBox permette la registrazione degli accessi da parte degli utenti ai file aziendali (attraverso l'audit su file server e NAS), ma anche di dimostrare che le modalità di cancellazione sicura dei dati personali eventualmente conservati siano rispettate.

ARTICOLO 17
("right to erasure/right to be forgotten")

- Monitoraggio degli accessi alle risorse da parte degli utenti (sistemi di autenticazione, accessi VPN, file server, NAS, server di posta eccetera);
- monitoraggio degli accessi alle risorse da parte degli amministratori di sistema (access log, dettagli riguardanti le operazioni svolte sui sistemi);
- monitoraggio dei log di traffico dei firewall perimetrali (informazioni sulle connessioni di rete che hanno origine dai sistemi interni, comunicazione con sistemi di Command and Control, identificazione di possibili azioni di data exfiltration);
- monitoraggio dei log generati dalle piattaforme di Endpoint Protection (EPP) e Endpoint Detection and Response (EDR), permettendo l'identificazione di malware o possibili attacchi rivolti a sottrarre dati aziendali;
- monitoraggio dei log generati da strumenti di Host Intrusion Prevention e Detection (IPS, IDS), anche host-based (HIDS);
- monitoraggio dei log generati dalle soluzioni di File Integrity Monitoring (FIM) e Data Leakage Protection (DLP) posti a protezione dei dati aziendali;
- riduzione della superficie d'attacco attraverso attività di vulnerability mangement (modulo NVS); identificazione delle vulnerabilità degli asset legate a mancati aggiornamenti o a configurazione non corrette (hardening); classificazione delle minacce;
- raccolta di Open Source Threat Intelligence Feed di terze parti (moduli LM e LCE) per ridurre il numero di falsi positivi e fornire informazioni certe al personale tecnico;
- avanzate funzioni di analisi e rappresentazione dei dati raccolti per facilitare il processo di gestione degli incidenti informatici.

Il modulo di Log Correlation Engine (LCE), sfruttando le informazioni raccolte, consente d'identificare scenari di rischio attraverso regole di correlazione in grado d'intraprendere contromisure automatiche.

ARTICOLO 24
("responsibility of the controller")

ARTICOLO 25
("data protection by design and by default")

ARTICOLO 28
("right to erasure/right to be forgotten")

SGBox consente di dimostrare l'adeguatezza delle proprie misure tecniche e organizzative attraverso la centralizzazione delle informazioni di sicurezza dei sistemi (firewall, IDS/IPS, EPP, EDR, DLP, FIM, VPN, directory service eccetera).

Un potente motore di riconoscimento e normalizzazione dei log, attraverso un'interfaccia semplice e intuitiva, permette all'utente di aggregare liberamente i log prodotti dalle varie piattaforme esistenti in azienda. I dati così raccolti potranno quindi essere analizzati e amministrati centralmente effettuando un'analisi in tempo reale oppure sullo storico dei log. I dati analizzati potranno essere rappresentati da una serie di grafici e report dettagliati e totalmente personalizzabili (dashboard).
Sarà possibile sfruttare i meccanismi di autenticazione di un directory server esterno per collegarsi alla web console SGBox, se necessario avvalendosi della strong authentication.

ARTICOLO 32
("Security of processing"); in particolar modo in riferimento alla necessità di adottare misure tecniche e organizzative adeguate)

SGBox favorisce l'individuazione delle violazioni dei sistemi (articoli 33 e 34), anche avvalendosi di funzionalità automatiche basate su modelli comportamentali di User Behavior analytics (UBA).
La piattaforma offre completa visibilità (24x7) degli eventi di sicurezza (dashboard, viste ecc.) al fine d'identificare un attacco e accelerare i tempi di risposta in caso d'incidente informatico.
La centralizzazione delle informazioni (con la possiblità d'impostare tempi di retention personalizzati, al fine di rispettare le esigenze di sicurezza dei sistemi, osservando il principio di proporzionalità) favorisce le indagini e permette di stabilire la possibile root cause di un data breach.

ARTICOLO 33
("notification of a personal data breach to the supervisory authority")

ARTICOLO 34
("communication of a personal data breach to the data subject")and by default")

SGBox offre la possibilità di differenziare l'accesso alle informazioni di log nel rispetto dei principi di least privilege e need to know. Ad esempio, se richiesto, SGBox permette di mascherare in visualizzazione (attraverso parser) le informazioni di navigazione degli utenti provenienti dai log di un proxy server, al fine di consentirne l'accesso al solo personale autorizzato (data obfuscation).
Con SGBox è possible applicare correttamente le tecniche di role-based access control (RBAC) per limitare l'accesso alle informazioni di log contenute nella piattaforma SIEM.
La piattaforma offre funzionalità di discovery degli asset e la definizione di gruppi dinamici di host legati a funzioni aziendali specifiche (sistemi a perimetro ISO 27001, sistemi dell'ufficio del personale eccetera).

ARTICOLO 35
("data protection impact assessment")

NEXT GENERATION SIEM

CONTATTACI

Via Melchiorre Gioia, 168
Milano - 20153 - Italia

+ 39 02 60830172

sales@sgbox.it

www.sgbox.it