Introduzione

La sempre maggior digitalizzazione delle imprese porta a un volume di dati raccolti e trattati da ogni azienda, sebbene in modo non sempre pienamente consapevole da ciascun utente, enorme e in continua crescita. Di pari passo sono aumentati esponenzialmente i rischi e i disastri informatici, furti di dati personali, casi di estorsione tramite "ransomware" e uso illecito dei dati stessi. Con la revisione della Legge federale sulla protezione dei dati (nLPD), dal 2023 cambiano alcune importanti disposizioni sul trattamento dei dati personali. Le aziende in futuro dovranno osservare regole più severe e dovrebbero pertanto modificare le loro attuali direttive e dichiarazioni sulla protezione dei dati entro l'entrata in vigore, che avverrà il primo settembre 2023.

Punti principali della revisione della Legge federale sulla protezione dei dati (nLPD):

1. **Campo di applicazione:** nLPD si limita alla protezione dei dati delle persone fisiche.
2. **Estensione maggiore:** ora anche i dati genetici e biometrici sono considerati degni di particolare protezione.
3. **Registro delle attività di trattamento:** le aziende hanno l'obbligo di tenere un registro delle attività di trattamento contenente le informazioni prescritte.
4. **Valutazioni d'impatto sulla protezione dei dati:** le aziende avranno l'obbligo di eseguire una valutazione d'impatto sulla protezione dei dati.
5. **Notifica tempestiva:** le violazioni della sicurezza dei dati dovranno essere notificate il più rapidamente possibile.
6. **Privacy by design e privacy by default:** obbliga le aziende a tenere conto dei principi generali del trattamento dei dati.

Come SGBox Supporta la Compliance LPD

Campo di applicazione

SGBox permette la raccolta e la gestione dei log di accesso al dato, permettendo così il monitoraggio delle operazioni effettuate su tali dati.

Lo strumento consente al cliente di impostare una politica di conservazione dei dati personalizzata per ogni tipo di registro. Il cliente può definire la retention specifica sia a livello globale che a livello singolo / gruppo di host. I dati raw log raccolti sono crittografati, firmati digitalmente, protetti, contrassegnati con data e ora e compressi.

La soluzione è in grado di archiviare i dati degli eventi nel suo formato originale per essere conforme alle regole governative come GDPR nLPD e altro. È possibile archiviare i log all'interno di SGBox o in uno storage esterno con funzioni di backup e restore.

Estensione maggiore

SGBox può raccogliere log da tutti i tipi di fonti di dati, tramite diverse metodologie (Syslog, wmi, sgbox light agent, file di testo, Trap SNMP, API, Query, Netflow, ecc...).

Registro delle attività di trattamento

SGBox permette la registrazione dei log di accesso, modifica o eliminazione dei dati. Questo consente un monitoraggio continuo e il mantenimento di uno storico delle attività che interessano tali dati.

Valutazioni d'impatto sulla protezione dei dati

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 possibile applicare correttamente le tecniche di role-based access control (RBAC) per limitare l'accesso alle informazioni di log contenute nella piattaforma SIEM.

Notifica tempestiva

SGBox favorisce l'individuazione delle violazioni dei sistemi, anche avvalendosi di funzionalità automatiche basate su modelli comportamentali di User Behavior analytics (UBA). La piattaforma offre completa visibilità (24×7) degli eventi di sicurezza (dashboard, viste ecc.) al fine d'identificare un attacco e accelerare i tempi di risposta in caso d'incidente informatico e di notifica. La risposta automatica consente azioni come allarme, e-mail, messaggi Telegram, esecuzione di script e chiamate API REST di terze parti.

Privacy by design e privacy by default

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.

- 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.

Sanzioni

La LPD svizzera punisce la mancata conformità con multe fino a 250.000 CHF. Consente inoltre di imporre sanzioni penali a soggetti privati responsabili di una potenziale violazione, ad esempio a titolari e responsabili del trattamento, e non solo alle aziende.