Informatica

White paper

Riduci i rischi di privacy dei dati per il Master Data Management

Informazioni su Informatica

La Digital Transformation cambia le nostre aspettative: migliori servizi, consegne più rapide, il tutto a costi più contenuti. Le aziende devono trasformarsi per rimanere competitive e i dati sono la risposta per riuscirci.

Siamo leader mondiali nell'Enterprise Cloud Data Management e siamo pronti a supportare la tua leadership intelligente in qualsiasi settore, categoria o nicchia di mercato. Informatica ti offre la possibilità di operare in un ambiente più agile, realizzare nuove opportunità di crescita o persino inventare cose nuove. Siamo focalizzati al 100% sui dati e questo ti offrirà la flessibilità necessaria per competere ed avere successo.

Ti invitiamo a scoprire tutto quello che Informatica ha da offrirti e a liberare "the power of data" per promuovere la tua prossima intelligent disruption.

Indice

Executive Summary

Per creare una vista affidabile e autorevole delle informazioni su clienti, prodotti e servizi, informazioni operative e altre informazioni di livello enterprise business-critical, le organizzazioni investono in iniziative di Master Data Management (MDM). L'MDM combina elementi relativi ai dati fondamentali di tutta l'azienda in record consolidati per creare dati affidabili da condividere con le persone e le applicazioni che ne hanno bisogno. Questo ha un enorme valore per qualsiasi azienda che intenda creare offerte più focalizzate sul cliente, migliorare il customer service e i programmi fedeltà, ottenere l'efficienza nella gestione dei prodotti e nelle soluzioni, migrare al Cloud in sicurezza e così via.

I dati affidabili diventano i "gioielli della corona" delle iniziative dell'organizzazione legate a clienti e prodotti e garantiscono un vantaggio competitivo. Tuttavia, il consolidamento dei dati sensibili costituisce anche un bersaglio invitante per attacchi esterni che portano a violazioni della sicurezza dei dati e aumenta il potenziale uso improprio interno, ed è pertanto soggetto a normative in materia di privacy, come ad esempio il regolamento generale sulla protezione dei dati (GDPR), il California Consumer Privacy Act (CCPA) e altre.

Sorgono spontanee domande sulla conformità e la protezione dei dati per questi ambienti:

- Dove sono ubicati tutti i dati e come proliferano?
- Che cosa alimenta il repository e chi accede ai dati e con quali applicazioni?
- L'attuale accesso e utilizzo rispetta le normative e le policy approvate sull'utilizzo dei dati?
- Le protezioni dei dati sono adeguate e il rischio legato ai dati resta a livelli accettabili o esistono condizioni che creano rischi non opportuni che devono essere corretti?

I risultati della discovery e della classificazione dei dati sensibili dei clienti sono diventati la base per supportare decisioni sul rischio, la protezione e la conformità alle normative dei dati master.

Questo white paper offre un framework di considerazioni e strategie per attenuare il rischio con una soluzione focalizzata sui dati che:

- Applica gli analytics, l'intelligence guidata dai metadati, l'automazione e l'intelligenza artificiale per identificare e proteggere i dati master sensibili
- Adempie alle normative in materia di data governance e privacy in costante evoluzione
- Garantisce la preparazione agli audit per dimostrare i controlli in atto e
- Avvisa gli stakeholder quando si verificano comportamenti anomali che richiedono un'indagine

Introduzione

Secondo la società di ricerca IDC, si prevede che nel mondo saranno creati 175 zettabyte di dati nel 2025, da 33 zettabyte nel 2018.[1] Le organizzazioni di tutti i settori si basano sull'accuratezza, la disponibilità e la protezione dei propri dati per generare fatturato, servire i clienti, aumentare la produttività, ottimizzare le attività e attuare altri processi di business mission-critical.

La continua crescita esponenziale del volume e dell'utilizzo dei dati comprende anche i dati master sensibili di diversi silos, sia on-premise che nel Cloud, e una vasta gamma di formati di dati. Tali condizioni hanno reso obsoleti i tradizionali metodi di sicurezza,[2] richiedendo un nuovo approccio alla sicurezza dei dati master in un'organizzazione.

Tuttavia, la maggior parte delle aziende non è in grado di identificare in modo preciso dove si trovano e da dove si accede a tutti i dati master sensibili, in particolare se sono in formato non strutturato. Questa scarsa visibilità aumenta il rischio per le organizzazioni e, di conseguenza, la violazione della sicurezza dei dati resta uno dei principali rischi per l'IT.[3]

Con l'aumento delle violazioni della sicurezza dei dati, accanto alla proliferazione dei dati master sensibili utilizzati in modo inappropriato, le organizzazioni devono sviluppare una strategia di attenuazione del rischio che comprenda una soluzione per la privacy data-centric con le seguenti caratteristiche principali:

- Visibilità su tutte le fonti dati in tutta l'organizzazione, per individuare e classificare i dati master sensibili
- Possibilità di implementare meccanismi di protezione per i dati master sensibili al fine di ridurre le violazioni della sicurezza dei dati
- Conformità alle attuali normative in materia di privacy, compreso l'utilizzo di intelligence guidata dai metadati, automazione e intelligenza artificiale per monitorare il comportamento degli utenti e segnalare le anomalie in tempo quasi reale
- Tool di visualizzazione analitica avanzati per la valutazione del rischio e la gestione dei dati sensibili
- Funzionalità di reporting trasparenti e complete per dimostrare i controlli con la preparazione per gli audit

Gartner prevede che i prodotti di protezione integrati sostituiranno i diversi tool di sicurezza dei dati in silos nel 40% delle grandi aziende (da meno del 5%).[4] Queste soluzioni di protezione data-centric offrono una vista centralizzata dei dati a rischio in modo che tutti gli stakeholder principali di un'organizzazione globale possano monitorare lo spostamento dei dati sensibili e applicare meccanismi di protezione come richiesto dalle policy di governance e dalle normative.

Una strategia in quattro step per attenuare il rischio per la privacy dei dati sensibili

Il rischio per la privacy dei dati sensibili è l'impatto della perdita di dati sensibili legato all'esposizione inappropriata, la cui causa più comune è la violazione dei dati o l'utilizzo interno improprio. Un equivoco diffuso è ritenere che sia sufficiente individuare i dati master sensibili per correggere il rischio. Tuttavia, l'individuazione e la classificazione di questi dati è solo il primo passaggio in una strategia completa di correzione dei rischi.

[1] IDC White Paper, "The Digitization of the World – From Edge to Core" (novembre 2018).
[2] Gartner, "Market Guide for Data-Centric Audit and Protection", 21 marzo 2017.
[3] Ponemon Institute LLC, "Data Breaches and Sensitive Data Risk", febbraio 2016.
[4] Gartner, "Market Guide for Data-Centric Audit and Protection", 21 marzo 2017.

I passaggi successivi comportano la valutazione delle priorità relative al rischio dell'organizzazione, in base ai risultati dell'analisi di individuazione e classificazione. Devi stabilire una strategia per ridurre i principali rischi, con controlli automatici che applicano le policy di data governance e coinvolgere tutti i principali stakeholder, non solo l'IT. La tua strategia dovrebbe includere l'implementazione di una soluzione per la protezione e la privacy data-centric e affidabile, in grado di offrire funzionalità per la conformità alle normative, comprese visualizzazioni analitiche avanzate dei dati sensibili per le dashboard di visibilità del rischio e reporting per gli audit dei controlli di conformità, nonché protezione per tutti i tipi di dati master sensibili in tutta l'organizzazione.

1. Discovery e classificazione

Un approccio comune ad hoc alla discovery prevede di esaminare le fonti esistenti e inviare questionari. Tuttavia, questo approccio manuale è inadatto, perché utilizza tempo e risorse preziosi, spesso risulta inaccurato e diventa rapidamente obsoleto, basandosi sul self-reporting anziché sull'effettivo monitoraggio del comportamento e del flusso di dati degli utenti in tempo reale.

Le organizzazioni si devono porre le seguenti domande:

- Quali dati archivi, chi vi ha accesso e a quale scopo?
- Come gestisci i privilegi degli utenti e assegni i diritti sui dati?
- Con quale grado di efficacia sei in grado di proteggere i dati master sensibili e garantire che siano applicati i controlli adeguati?

Tra le altre considerazioni per la conformità a livello di discovery e classificazione troviamo:

- Definire e comprendere il panorama legato ai dati, compresi database e dati non strutturati
- Mappare i sistemi che contengono dati sensibili gestiti
- Cercare una soluzione in grado di mappare lo spostamento di questi dati in tutto l'ecosistema mantenendo al tempo stesso una vista in tempo quasi reale con tool di analytics e reporting

2. Conformità

Le organizzazioni faticano a identificare, monitorare e correggere i rischi legati ai dati per adempiere alle normative in materia di privacy dei dati. Inoltre devono monitorare, analizzare e inviare avvisi sui casi di accesso o spostamento dei dati che possono mettere a rischio la conformità.

Il GDPR, in vigore dal 25 maggio 2018, è stato adottato con l'obiettivo di rafforzare e unificare la protezione dei dati per tutti i cittadini all'interno dell'UE, semplificando l'ambiente normativo per le aziende internazionali. Analogamente, il CCPA, in vigore dall'1 gennaio 2020, innalza gli standard, estendendo la privacy fino a includere i dati sul nucleo familiare.

Molte aziende non sono ancora del tutto pronte per queste normative e non sono adeguatamente conformi; la non conformità potrebbe comportare pesanti sanzioni e danni alla reputazione. D'altro canto, la conformità può garantire un vantaggio competitivo come fattore di differenziazione in tema di privacy dei dati master aumentando la customer loyalty e favorendo al tempo stesso l'ottenimento dei risultati della digital transformation. Inoltre, le aziende che si dimostrano impegnate nella protezione dei dati possono ottenere 5 volte più facilmente l'accesso alle informazioni personali dai clienti che si fidano della loro gestione responsabile.[5]

[5] Excerpt, Boston Consulting Group, "Bridging the Trust Gap in Personal Data"

Le organizzazioni devono sviluppare policy intelligenti per identificare gli store di dati che contengono "domini di dati" correlati al GDPR, al CCPA e ad altre normative simili in materia di privacy. Tali policy devono essere multifattoriali e provviste di logica di data intelligence per stabilire quali combinazioni rappresentano una minaccia di esposizione a rischi per la privacy.

3. Protezione

Nel terzo trimestre del 2019, sono state registrate oltre 5.000 violazioni dei dati, con quasi 8 miliardi di record esposti.[6] Naturalmente, malgrado forti investimenti in privacy e sicurezza dei dati, i dati personali restano vulnerabili. Le organizzazioni devono continuamente proteggere i dati ad alto rischio, identificare i comportamenti sospetti e l'utilizzo o lo spostamento non autorizzato, automatizzando e orchestrando al tempo stesso le misure di correzione.

Le organizzazioni dovrebbero assegnare la priorità ai più importanti rischi legati ai dati e correggere tali rischi con controlli focalizzati sui dati che supportino la mobilità dei dati, anziché affidarsi soltanto ai tradizionali controlli degli accessi al server, firewall e tool di cybersicurezza focalizzati sul sistema. Ad esempio, i controlli focalizzati sui dati comprendono mascheramento, controllo basato sulle identità e crittografia.

Oltre ai controlli relativi alla privacy dei dati, le organizzazioni devono monitorare l'accesso ai dati e il comportamento in base all'identità. Un accesso eccessivo o un comportamento insolito possono indicare che gli utenti non rispettano le policy di privacy o che le credenziali degli utenti sono state compromesse.

4. Preparazione e risposta agli audit

Le aziende sono sottoposte più che mai a audit e valutazioni dei dati sensibili. Faticano a fornire agli auditor prova del fatto che hanno visibilità sui dati fondamentali e che ne garantiscono la protezione.

Le organizzazioni dovrebbero essere in grado di rispondere agli auditor in modo immediato e dimostrare che sanno dove si trovano i dati, quali sono i relativi rischi, come vengono protetti e come vengono utilizzati i dati. Dovrebbero considerare che gli auditor vogliono report e visualizzazioni astratte per dipartimenti o sedi e che permettano di approfondire domini di dati specifici.

Conclusione

Il potere dell'MDM può aiutare le organizzazioni a trasformare attività e servizi. Il potere di questi dati è chiaro, ma rappresenta anche un bersaglio invitante per l'utilizzo improprio da parte di attori interni o esterni. Se questo si abbina all'assalto continuo rappresentato da data breaches e crescenti requisiti di conformità, le organizzazioni devono ripensare i propri processi e tool per identificare, analizzare e proteggere i dati sensibili.

Nell'attuale clima di aumento dei rischi per la privacy e di continue violazioni dei dati, le aziende devono sviluppare subito una strategia digitale solida per monitorare, analizzare e correggere in modo costante il rischio per i propri dati master sensibili. Devono monitorare i dati in tempo quasi reale per rilevare segnali di utilizzo improprio o violazione della sicurezza dei dati, accesso o comportamento insolito o impropri trasferimenti oltre frontiera. Con questo impegno, le organizzazioni possono utilizzare al meglio l'MDM e migliorare la propria posizione rispetto al rischio legato ai dati per contribuire ad attenuare l'impatto delle violazioni dei dati o dell'utilizzo improprio a livello interno e soddisfare i rigorosi requisiti delle normative specifiche per area geografica e settore.

[6] Risk Based Security: Q3 2019 Data Breach QuickView Report

Consigli

1. Esegui una valutazione del rischio di privacy dei dati per ottenere una comprensione chiara di dove si trovano i tuoi dati master sensibili, di come proliferano nel tuo ecosistema di dati e di quali insiemi di dati sensibili sono più vulnerabili.
2. In base ai risultati della tua valutazione, assegna la priorità alle fonti principali dei dati master più sensibili della tua azienda; stabilisci una strategia e individua una scadenza per proteggerle; infine implementa questa strategia come soluzione pilota per il tuo approccio alla privacy e protezione dei dati.
3. Definisci, documenta e distribuisci le policy di conformità alla privacy della tua organizzazione e individua gli stakeholder responsabili della conformità alle normative in materia di privacy. Crea un piano strategico per quest'anno e oltre.

Ulteriori ricerche

Per maggiori informazioni sui rischi legati alla sicurezza e alla protezione dei dati sensibili, consulta le seguenti pubblicazioni e i seguenti video:

Informatica Data Privacy Management

Informatica Master Data Management – Customer 360

White paper: Intelligent Data Privacy

Bloor Research: Discovering Sensitive Data

Sede centrale mondiale Piazza della Repubblica 14/16, 20124 Milano Tel: +39 02 37 05 80 00 |
Via Luca Gaurico 9/11, 00143 Roma Tel: +39 06 54 83 21 31 Numero verde negli Stati Uniti: 1.800.653.3871

IN09_0520_03409