Informatica

White paper

Sicurezza data-centric per un mondo ibrido

La conformità al GDPR in ambienti Cloud e on-premise

Informazioni su Informatica

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

Quale leader mondiale nell'Enterprise Cloud Data Management, possiamo supportarti per evolvere in modo intelligente in qualsiasi settore, categoria o nicchia di mercato. Informatica ti offre la possibilità di diventare 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 4

Sicurezza dei dati per la tua realtà ibrida 5

Una strategia in quattro punti per la protezione dei dati sensibili 6

1. Discovery e classificazione 6

2. Conformità 7

3. Protezione 7

4. Preparazione e risposta agli audit 7

Conclusione 8

Consigli 8

Ulteriori informazioni 8

Executive Summary

Oggi la maggior parte delle organizzazioni archivia dati sensibili su clienti, prodotti e altri dati fondamentali in un numero crescente e sempre più diversificato di piattaforme e posizioni fisiche in tutto il mondo. Questi dati business-critical spesso si trovano in applicazioni di Cloud pubblico, on-premise e Software as a Service (SaaS). Con Informatica Intelligent Cloud Services™, ad esempio, Informatica fornisce sicurezza per l'infrastruttura sotto forma di data center di failover, autenticazione degli utenti e controllo degli accessi, protocolli di sicurezza di rete, crittografia e layer di sicurezza a livello di sistema operativo, database e applicazione.[1]

Gli ambienti ibridi presentano nuove sfide ai team addetti alla conformità dei dati e alla sicurezza. La natura dinamica di dati, utenti e applicazioni richiede misure aggiuntive per garantire che i dati fondamentali dell'organizzazione siano sempre monitorati, compresi e protetti. I rischi non sono ipotetici, come dimostrato dalle violazioni ad alto profilo a livello di ambienti Cloud e on-premise e dalle sanzioni derivanti dalle nuove normative come ad esempio il regolamento generale sulla protezione dei dati (GDPR).

In questi ambienti ibridi dinamici l'intelligence e l'automazione sono necessarie per garantire protezione dei dati e conformità costanti, con la possibilità di rispondere a domande come le seguenti:

- Dove sono tutti i dati che è necessario proteggere?
- Chi accede ai dati e con quali applicazioni?
- L'attuale accesso e utilizzo rispetta le normative e le policy 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 più rischi di quelli che dovremmo correggere?

I risultati della discovery e della classificazione dei dati sensibili sono diventati la base per supportare decisioni sul rischio legato ai dati, la sicurezza e la conformità in un ecosistema di dati ibrido. Questo documento offre un quadro di considerazioni e strategie relative alla sicurezza negli ambienti ibridi, con un approccio focalizzato sui dati che può:

- Applicare gli analytics, l'automazione e l'intelligenza artificiale (AI) per identificare e proteggere i dati sensibili provenienti da tutte le fonti in un ambiente ibrido, utilizzando un'unica interfaccia per dashboard e reporting.
- Adempiere alle normative in materia di data governance e sicurezza in costante evoluzione.
- Garantire la preparazione agli audit.
- Avvisare i principali stakeholder quando si verificano comportamenti anomali.

Informatica Data Masking e Informatica Secure@Source® offrono eccellenti funzionalità per eseguire queste funzioni, aggiungendo un layer di sicurezza integrato e focalizzato sui dati per tutte le fonti di dati sensibili in un ecosistema ibrido.

[1] Monahan, David, "Informatica Cloud Security Architecture Overview", Enterprise Management Associates (EMA), marzo 2016.

Sicurezza dei dati per la tua realtà ibrida

Secondo la società di ricerca IDC, si prevede che nel mondo saranno creati 180 zettabyte di dati nel 2025, da meno di 10 zettabyte nel 2015.[2] Le organizzazioni di tutti i settori si basano sull'accuratezza, la disponibilità e la sicurezza dei propri dati per creare profitto, servire i clienti, aumentare la produttività e supportare altri processi di business mission-critical.

La continua crescita esponenziale del volume e dell'utilizzo dei dati comprende anche i dati 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, richiedendo un nuovo approccio alla sicurezza dei dati in un'organizzazione.[3]

Inoltre, seguendo un trend consolidato, una percentuale elevata dei dati utilizzati dalle organizzazioni proviene da fonti esterne. È fondamentale comprendere la sensibilità di questi dati al momento in cui avviene l'onboarding nell'organizzazione, e prima che i dati vengano distribuiti nei diversi sistemi e analytics. Tuttavia la maggior parte delle aziende non è in grado di identificare in modo preciso dove si trovano i dati sensibili, in particolare se sono in formati non strutturati o su applicazioni on-premise e Cloud, database relazionali, appliance di data warehouse e fonti di Big Data differenti. Questa scarsa conoscenza aumenta il rischio per le organizzazioni. Di conseguenza, attualmente il principale rischio di sicurezza IT è rappresentato dalle violazioni dei dati.[4]

Con l'aumento delle violazioni dei dati, che va di pari passo con la proliferazione dei dati sensibili, le organizzazioni devono sviluppare una strategia di attenuazione dei rischi che comprenda un prodotto per la sicurezza data-centric con le seguenti caratteristiche principali:

- Visibilità su tutte le fonti dati per individuare e classificare i dati sensibili di tutta l'organizzazione.
- Possibilità di implementare meccanismi di protezione per i dati sensibili al fine di ridurre le violazioni.
- Conformità alle attuali normative in materia di sicurezza e privacy dei dati, compreso l'utilizzo di 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 gestione dei dati sensibili.
- Funzionalità di reporting trasparenti e solide per la preparazione agli audit.

Gartner prevede che entro il 2020 i prodotti per gli audit e la protezione focalizzati sui dati sostituiranno i diversi tool di sicurezza dei dati in silos nel 40% delle grandi aziende, da meno del 5% oggi.[5] Queste soluzioni di protezione data-centric, tra cui Informatica Data Masking e Informatica Secure@Source, offrono una vista centralizzata dei dati a rischio, per consentire a tutti gli stakeholder principali di un'organizzazione di monitorare lo spostamento dei dati sensibili e applicare meccanismi di protezione, come richiesto dalle policy e dalle normative di governance.

[2] "2016 IoT Midyear Review – The Report Card for Everyone", IDC, 4 agosto 2016.
[3] "Market Guide for Data-Centric Audit and Protection", Gartner, 21 marzo 2017.
[4] "Data Breaches and Sensitive Data Risk", Ponemon Institute, febbraio 2016.
[5] "Market Guide for Data-Centric Audit and Protection", Gartner, 21 marzo 2017.

Una strategia in quattro punti per la protezione dei dati sensibili

Il "rischio legato ai dati sensibili" è l'effetto della perdita di dati sensibili e la principale causa di tale perdita è rappresentato da una violazione dei dati. Un equivoco diffuso è ritenere che sia sufficiente individuare i dati 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.

I passaggi successivi comportano la valutazione del rischio dell'organizzazione in base ai risultati dell'analisi di individuazione e classificazione e la determinazione di una strategia per ridurre il rischio che coinvolga tutti i principali stakeholder, non solo l'organizzazione IT, con controlli automatici che applicano le policy di data governance. La tua strategia dovrebbe prevedere anche la ricerca e l'implementazione di un prodotto per la sicurezza data-centric solido, in grado di offrire funzionalità per la conformità alle normative, visualizzazioni analitiche avanzate dei dati sensibili per dashboard e reporting per gli audit e protezione per tutti i tipi di dati sensibili in tutta l'organizzazione. Il prodotto per la sicurezza data-centric scelto deve inoltre proteggere i dati sensibili provenienti da tutte le fonti del tuo ambiente ibrido: Cloud pubblico, applicazioni SaaS, applicazioni e database on-premise, dati non strutturati e appliance di data warehouse.

1. Discovery e classificazione

Un approccio comune alla discovery prevede di esaminare le fonti esistenti e inviare questionari. Tuttavia questo approccio molto manuale è inadeguato, perché utilizza tempo e risorse preziosi e spesso risulta inaccurato e obsoleto, basandosi sul self-reporting anziché sull'effettivo monitoraggio del comportamento degli utenti.

Le organizzazioni devono porsi le seguenti domande:

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

Altre iniziative importanti per la conformità a livello di discovery e classificazione:

- Definire e comprendere il panorama dei dati (compresi database, applicazioni e dati non strutturati on-premise e nel Cloud).
- Creare un piano per gestire i dati provenienti da fonti esterne.
- Mappare i sistemi che contengono dati sensibili.
- Cercare una soluzione in grado di mappare lo spostamento dei 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 e sicurezza 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'Unione europea, semplificando l'ambiente normativo per le aziende internazionali. Molte aziende non sono ancora pronte per questo regolamento e non dispongono di un grado di conformità adeguato; 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 e sicurezza dei dati sensibili, favorendo al tempo stesso l'ottenimento dei risultati della digital transformation guidata dai dati.

Le organizzazioni devono sviluppare policy intelligenti per identificare gli store di dati che contengono "domini di dati" correlati al GDPR. Tali policy devono essere multifattoriali e provviste di logica per stabilire quali combinazioni rappresentano una minaccia alla privacy.

3. Protezione

Nel 2017 sono state rilevate 1120 violazioni dei dati, con un totale di 171 milioni di record esposti.[6] Chiaramente, nonostante gli ingenti investimenti nella sicurezza a livello di infrastruttura, i dati fondamentali rimangono vulnerabili. Le organizzazioni devono proteggere continuamente i dati ad alto rischio, identificare i comportamenti sospetti e l'utilizzo o lo spostamento non autorizzato delle risorse di dati fondamentali, nonché automatizzare e orchestrare la correzione.

Le organizzazioni dovrebbero identificare i rischi legati ai dati fondamentali e correggerli con controlli focalizzati sui dati (anziché con i classici tool di cybersicurezza). Ad esempio, controlli che includano soluzioni di data masking e crittografia. Inoltre, dovrebbero monitorare l'accesso e il comportamento degli utenti. Un accesso eccessivo ai dati o un comportamento insolito possono indicare che gli utenti non rispettano le policy di privacy o che le loro credenziali sono state rubate.

4. Preparazione e risposta agli audit

Le aziende sono sottoposte più che mai a audit e valutazioni dei dati sensibili. Spesso faticano a dimostrare agli auditor 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, come vengono protetti, come vengono utilizzati e quali sono i rischi connessi ai dati. Dovrebbero considerare che gli auditor vogliono report e visualizzazioni astratte per dipartimenti o sedi e che permettano di approfondire domini di dati specifici.

[6] "2016 Data Breach Category Summary", Identity Theft Resource Center, 31 dicembre 2016.

Conclusione

Sono necessari protocolli di sicurezza dell'infrastruttura di livello superiore, per proteggere qualsiasi ambiente ibrido che trasmette dati riservati a utenti, server di data center in tutto il mondo e applicazioni Cloud. Il volume crescente di violazioni dei dati ma anche di requisiti di conformità indica che le organizzazioni devono implementare processi e tool adeguati per identificare, analizzare e proteggere i dati sensibili.

Nell'attuale clima di aumento dei rischi per la sicurezza e di continue violazioni dei dati, le aziende devono sviluppare una strategia di sicurezza digitale solida per monitorare, analizzare e correggere in modo costante i rischi per i propri dati sensibili. Devono monitorare i dati in tempo quasi reale per rilevare segnali di utilizzo improprio o violazione, accesso eccessivo, comportamento insolito o trasferimenti oltre frontiera. Con soluzioni di sicurezza data-centric come ad esempio Informatica Data Masking e Informatica Secure@Source, le organizzazioni possono 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.

Consigli

1. Esegui una valutazione del rischio, per ottenere una comprensione chiara di dove si trovano i tuoi dati sensibili, quanto si propagano nel tuo ecosistema di dati e quali insiemi di dati sensibili sono più vulnerabili.
2. In base ai risultati della tua valutazione, assegna la priorità alle dieci fonti principali dei dati più sensibili della tua azienda; stabilisci una strategia e individua un prodotto per proteggerle; infine implementa la strategia per la sicurezza dei dati.
3. Definisci, documenta e distribuisci le policy di conformità della tua organizzazione agli stakeholder responsabili della conformità al GDPR. Crea un piano strategico per maggio 2018 e oltre.

Ulteriori informazioni

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

- "Rilevamento e protezione: un approccio data-centric alla sicurezza dei dati", Informatica, aprile 2017.
- "Data Breaches and Sensitive Data Risk", Ponemon Institute, febbraio 2016.

Informatica

Piazza della Repubblica 14/16 - 20124 Milano, Italia. Tel: +39 02 37 05 80 00 | Via Luca Gaurico 9/11 - 00143 Roma, Italia. Tel: +39 06 54 83 21 34

IN09_0418_03429