Informatica

White Paper

Verringerung des Datenschutzrisikos beim Master Data Management

Informationen zu Informatica

Die digitale Transformation verändert unsere Erwartungshaltung hin zu besserem Service und schnellerer Lieferung zu geringeren Kosten. Unternehmen müssen sich neu orientieren, um wettbewerbsfähig zu bleiben. Dabei spielen Daten eine zentrale Rolle.

Als führender Anbieter für Enterprise Cloud Data Management unterstützt Informatica Sie dabei, sich als intelligenter Vorreiter zu etablieren – völlig unabhängig davon, in welcher Branche, Kategorie oder Nische Sie tätig sind. Wir ermöglichen es Ihnen, flexibler zu werden, neue Wachstumsmöglichkeiten wahrzunehmen und Innovationen voranzutreiben. Informatica ist zu 100 % auf Daten fokussiert, und bietet Unternehmen vielseitige Lösungen, um sich am Markt durchzusetzen.

Entdecken Sie jetzt das gesamte Angebot von Informatica, um das komplette Potenzial Ihrer Daten zu nutzen und so die nächste intelligente Innovation auf den Weg zu bringen.

Inhaltsverzeichnis

Zusammenfassung 4

Einleitung 5

Ein 4-Punkte-Plan zur Verringerung des Datenschutzrisikos, dem sensible Daten ausgesetzt sind 5

- Ermittlung und Klassifizierung 6
- Compliance 6
- Schutz 7
- Audits 7

Schlussfolgerungen 7

Empfehlungen 8

Zusammenfassung

Unternehmen investieren in Master Data Management-Initiativen (MDM), um eine zuverlässige, aussagekräftige Sicht auf Kunden-, Produkt-, Service-, Betriebs- und andere geschäftskritische Unternehmensdaten zu erstellen. Mithilfe von MDM lassen sich wichtige Daten unternehmensweit in konsolidierten Datensätzen zusammenfassen, um zuverlässige Daten zu schaffen, die für die Nutzer und Anwendungen freigegeben werden können, die diese benötigen. Dadurch entstehen für Unternehmen, die ihre Kunden in den Mittelpunkt stellen, den Kundenservice und Treueprogramme verbessern, ihr Produktangebot effizienter gestalten, sicher in die Cloud migrieren und viele weitere Projekte umsetzen möchten, zahlreiche Vorteile.

Nichts ist bei Kunden- und Produktinitiativen so wichtig wie zuverlässige Daten, die zu Wettbewerbsvorteilen führen. Doch die Konsolidierung sensibler Daten stellt auch ein attraktives Ziel für Cyberangriffe dar, was zu Verstößen gegen die Datensicherheit führt und möglicherweise auch zu Missbrauch durch Insider. Daher sind zahlreiche Datenschutzvorschriften einzuhalten, wie die Datenschutz-Grundverordnung (DSGVO) oder das Gesetz California Consumer Privacy Act (CCPA).

Dadurch ergeben sich verschiedene Fragen für Datenschutz und Compliance für diese Umgebungen:

- Wo befinden sich all die Daten und wie werden sie verbreitet?
- Woher stammen die Daten, die ins Repository gelangen, und wer greift mit welchen Anwendungen auf welche Daten zu?
- Werden aktuelle Zugriffsbeschränkungen und Verwendung von Daten den Vorgaben rechtlicher Vorschriften und Richtlinien zur Datennutzung gerecht?
- Werden Daten angemessen geschützt und ist das verbleibende Risiko vertretbar, oder gibt es Faktoren, die das Risiko in unangemessener Weise erhöhen und deshalb beseitigt werden sollten?

Die Ergebnisse der Ermittlung und Klassifizierung sensibler Kundendaten dienen als Entscheidungsgrundlage hinsichtlich des Risikos, des Schutzes und Compliance mit Datenschutzvorschriften von MDM-Daten.

In diesem White Paper wird ein Framework mit Aspekten und Strategien zur Risikominderung mit einer datenbasierten Lösung vorgestellt, das folgende Vorteile bietet:

- Nutzung von Analytics, metadatenbasierter Intelligence, Automatisierung und KI zur Erkennung und zum Schutz sensibler MDM-Daten
- Compliance mit neuen Vorschriften für Data Governance und Datenschutz
- Erfüllung von Audit-Vorgaben, um nachzuweisen, welche Kontrollen verwendet werden
- Inkenntnissetzung von Stakeholdern, wenn verdächtiges Nutzerverhalten auftritt, das untersucht werden muss

Einleitung

Laut IDC werden 2025 weltweit schätzungsweise 175 Zettabytes an Daten erstellt. 2018 betrug diese Zahl noch 33 Zettabytes.[1] Unternehmen in sämtlichen Branchen verlassen sich auf Genauigkeit, Verfügbarkeit und Schutz ihrer Daten, um Umsatz zu generieren, Kunden zu betreuen, die Produktivität zu erhöhen, Abläufe zu optimieren und weitere, geschäftskritische Geschäftsprozesse zu unterstützen.

Aufgrund des exponentiellen Anstiegs des Datenvolumens und der Datennutzung finden sich auch sensible Stammdaten in verschiedenen Datensilos wieder, sowohl On-Premise als auch in der Cloud, und zwar in verschiedenen Formaten. Das führt dazu, dass herkömmliche Methoden zur Datensicherheit veraltet sind[2] und ein neuer Ansatz erforderlich ist, um Stammdaten unternehmensweit zu schützen.

Doch die meisten Unternehmen können nicht zuverlässig ermitteln, wo genau sich all ihre sensiblen Stammdaten befinden und wo sie abgerufen werden, insbesondere, wenn sie in einem unstrukturierten Format gespeichert werden. Durch diese fehlende Transparenz steigt das Risiko für Unternehmen. Daher gehören Verstöße gegen den Datenschutz immer noch zu den größten IT-Sicherheitsrisiken.[3]

Da die Anzahl an Verstößen gegen den Datenschutz steigt und sensible Daten immer öfter auf unangemessene Weise verbreitet werden, müssen Unternehmen eine Strategie zur Risikoverringerung entwickeln, die datenzentrischen Schutz mit folgenden Funktionen bietet:

- Transparenz aller Datenquellen, um sensible Stammdaten im gesamten Unternehmen zu ermitteln und zu klassifizieren
- Umsetzung von Schutzmechanismen für sensible Stammdaten, um Verstöße gegen die Datensicherheit zu minimieren
- Compliance mit aktuellen Vorschriften zum Datenschutz, einschließlich der Nutzung von metadatenbasierter Intelligence, Automatisierung und KI, um das Nutzerverhalten zu überwachen und Anomalien nahezu in Echtzeit zu melden
- Umfassende Tools zur visuellen Darstellung für die Risikobewertung und das Management sensibler Daten
- Transparente und umfassende Reporting-Funktionen, um Audit-Vorgaben gerecht zu werden und den Einsatz von Kontrollen nachzuweisen

Gartner rechnet damit, dass einzelne, fragmentierte Tools zur Sicherstellung der Datensicherheit bis in 40 Prozent der großen Unternehmen durch integrierte Schutzlösungen ersetzt werden. Heute liegt diese Zahl bei weniger als fünf Prozent.[4] Diese datenzentrischen Schutzlösungen bieten eine zentrale Ansicht gefährdeter Daten, so dass alle wichtigen Stakeholder eines Unternehmens die Verschiebung sensibler Daten nachverfolgen und Kontrollmechanismen umsetzen können, die aufgrund gesetzlicher Richtlinien und Vorschriften erforderlich sind.

Ein 4-Punkte-Plan zur Verringerung des Datenschutzrisikos, dem sensible Daten ausgesetzt sind

Bei dem Datenschutzrisiko, dem sensible Daten ausgesetzt sind, geht es um die Auswirkungen, die der Verlust sensibler Daten durch eine unsachgemäße Offenlegung hat. Die Hauptgründe dafür sind oft Verstöße gegen den Datenschutz oder Missbrauch durch Insider. Oftmals wird fälschlicherweise davon ausgegangen, dass das Risiko schon beseitigt werden kann, indem ermittelt wird, wo genau sich sensible Stammdaten befinden. Doch Ermittlung und Klassifizierung dieser Daten stellen nur den ersten Schritt einer umfassenden Strategie zur Risikominderung dar.

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

Die nächsten Schritte beinhalten die Einschätzung des Risikos, dem Ihr Unternehmen aufgrund der Speicherort- und Klassifizierungsanalyse ausgesetzt ist. Dabei wird ermittelt, welche Prioritäten zuerst behandelt werden müssen. Sie müssen eine Strategie zur Risikominderung festlegen, um die größten Risiken zu verringern. Diese Strategie sollte automatisierte Zugriffsbeschränkungen umfassen, um Data-Governance-Richtlinien umzusetzen, und alle wichtigen Stakeholder einbinden – und nicht nur die IT. Zudem sollte Ihre Strategie die Umsetzung einer zuverlässigen, datenbasierten Lösung für Datenschutz und -sicherheit beinhalten und Funktionen für Compliance mit gesetzlichen Vorschriften bieten, darunter auch detaillierte Visualisierungen von Analytics-Ergebnissen sensibler Daten in Form von Dashboards zur Transparenz und Audit Reporting von Compliance-Kontrollmechanismen sowie Schutz der gesamten, sensiblen, verwalteten Datentypen des Unternehmens.

1. Ermittlung und Klassifizierung

Ein gängiger Ad hoc-Ansatz zur Ermittlung von Daten besteht darin, vorhandene Datenquellen zu prüfen und Fragebögen zu versenden. Doch ein manueller Ansatz ist ungeeignet, da er zu ressourcen- und zeitintensiv ist und oftmals ungenaue und veraltete Ergebnisse liefert. Zudem verlässt er sich auf Selbsteinschätzungen und -berichte, anstatt dass das Verhalten von Nutzern und Datenflüsse in Echtzeit überwacht werden.

Unternehmen müssen sich folgende Fragen stellen:

- Welche Daten werden gespeichert, wer hat Zugriff darauf und für welche Zwecke?
- Wie werden Nutzerberechtigungen und Rechte zur Bereitstellung von Daten verwaltet?
- Wie werden sensible MDM-Daten geschützt und wie wird sichergestellt, dass angemessene Kontrollmechanismen genutzt werden?

Desweiteren spielen folgende Aspekte für Ermittlung und Klassifizierung eine Rolle:

- Definition und Verständnis der Datenlandschaft, einschließlich Datenbanken und unstrukturierter Daten
- Zuordnung, welche Systeme sensible MDM-Daten enthalten und Zuordnung dieser Daten zu Identitäten
- Anschaffung einer Lösung, die Data Lineage im gesamten Ökosystem zuordnen kann und gleichzeitig mithilfe von Analytics und Reporting Tools eine Datenansicht nahezu in Echtzeit bietet

2. Compliance

Es fällt Unternehmen schwer, Datenrisiken zu identifizieren, zu überwachen und zu beseitigen, um Datenschutzvorgaben gerecht zu werden. Zudem müssen sie Datenzugriffe oder Datenverschiebungen überwachen, analysieren und melden, die die Compliance gefährden könnten.

Die DSGVO ist am 25. Mai 2018 in Kraft getreten, und verfolgt das Ziel, den Datenschutz für alle Einzelpersonen in der Europäischen Union zu stärken und zu vereinheitlichen, wodurch auch die gesetzlichen Vorgaben für den internationalen Handel vereinfacht werden. In ähnlicher Weise erhöht auch das US-Gesetz CCPA, das am 1. Januar 2020 in Kraft getreten ist, den Datenschutz, der auf Haushaltsdaten erweitert wird.

Viele Unternehmen sind noch nicht ausreichend auf diese Vorschrift vorbereitet, obwohl Non-Compliance zu empfindlichen Geldstrafen und Rufschädigung führen kann. Compliance stellt zudem einen wichtigen Wettbewerbsvorteil für Unternehmen dar, da MDM und Datenschutz zu höherer Kundentreue führen und gleichzeitig die datenbasierte, digitale Transformation effizienter vorantreiben. Zudem profitieren Unternehmen, die Daten nachweislich sorgfältig schützen, davon, dass sie auf 5 Mal mehr personenbezogene Daten ihrer Kunden zugreifen können, da diese darauf vertrauen, dass die Verwendung verantwortungsvoll erfolgt.[5]

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

Unternehmen müssen intelligente Richtlinien entwickeln, um Data Stores zu identifizieren, die „Datendomänen" enthalten, die den Vorgaben der DSGVO, CCPA und ähnlichen Vorschriften unterliegen. Diese Richtlinien beinhalten mehrere Faktoren sowie eine Data Intelligence-Logik, die festlegt, welche Kombinationen eine Gefährdung des Datenschutzes darstellen.

3. Schutz

Im 3. Quartal 2019 wurden mehr als 5.000 Verstöße gegen den Datenschutz verzeichnet, wobei fast 8 Mrd. Datensätze offengelegt wurden.[6] Das zeigt, dass personenbezogene Daten trotz großer Investitionen in Datenschutz und -sicherheit immer noch nicht ausreichend geschützt werden. Unternehmen müssen Daten mit hohem Risiko kontinuierlich schützen, verdächtiges Verhalten, unbefugte Verwendung oder Verschiebung von Daten erkennen und die Risikominderung automatisieren und orchestrieren.

Dazu müssen Unternehmen die wichtigsten Datenrisiken priorisieren und mithilfe datenbasierter Kontrollmechanismen verringern, die Datenmobilität unterstützen, anstatt sich nur auf traditionelle Zugriffsbeschränkungen für Server, Firewalls und ähnliche, systemzentrische Cybersecurity Tools zu verlassen. Zu datenbasierten Kontrollmechanismen zählen beispielsweise Masking, identitätsbezogene Kontrollen und Verschlüsselung.

Zusätzlich zu Kontrollmöglichkeiten für den Datenschutz sollten Unternehmen den identitätsbasierten Datenzugriff und das Verhalten von Nutzern überwachen. Übermäßiger Datenzugriff oder ungewöhnliches Verhalten können darauf hinweisen, dass Nutzer sich nicht an Datenschutzrichtlinien halten oder dass ihre Zugangsdaten gestohlen wurden.

4. Audits

Die sensiblen Daten von Unternehmen sind heutzutage öfter Gegenstand von Audits und Bewertungen als je zuvor. Es fällt Unternehmen schwer, bei Audits nachzuweisen, dass ihre geschäftskritischen Daten transparent sind und geschützt werden.

Unternehmen sollten in der Lage sein, bei Audits umgehend nachzuweisen, dass sie genau wissen, wo sich ihre Daten befinden, welche Risiken bestehen und wie die Daten geschützt und verwendet werden. Sie müssen darauf vorbereitet sein, Berichte und Visualisierungen einzureichen, die für Abteilungen und Standorte abstrahiert wurden und zeigen, dass es möglich ist, spezifische Datendomänen detaillierter zu analysieren.

Schlussfolgerungen

Mithilfe von MDM können Unternehmen ihre Abläufe und Services optimieren. Der geschäftliche Nutzen dieser Daten ist unumstritten, doch sie stellen auch ein beliebtes Ziel für interne bzw. externe Angriffe dar. Diese Tatsache sowie die Zahl der Verstöße gegen den Datenschutz und die steigenden Compliance-Anforderungen verdeutlichen, dass Unternehmen angemessene Prozesse und Tools für Identifizierung, Analyse und Schutz sensibler Daten umsetzen müssen.

Angesichts des hohen Datenschutzrisikos und zahlreicher Verstöße gegen den Datenschutz müssen Unternehmen eine robuste, digitale Sicherheitsstrategie entwickeln, um ihre sensiblen Stammdaten permanent zu überwachen, zu analysieren und Risiken zu verringern. Sie müssen Daten nahezu in Echtzeit überwachen, um Signale zu erkennen, die auf eine missbräuchliche Verwendung oder Verstöße, ungewöhnlichen Zugriff und Nutzerverhalten oder unangemessenen grenzüberschreitenden Datentransfer hinweisen. Mit solchen Schutzmaßnahmen können Unternehmen MDM optimal nutzen und das Datenrisiko verringern, um Verstöße gegen den Datenschutz oder Fälle interner, missbräuchlicher Verwendung zu reduzieren und um den strikten Vorgaben regionaler und branchenweiter Vorschriften gerecht zu werden.

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

Empfehlungen

1. Führen Sie eine Risikobewertung durch, um genau zu verstehen, wo sich Ihre sensiblen MDM-Daten befinden, wie weit sie in Ihrem Daten-Ökosystem verteilt werden und welche sensiblen Datensätze am stärksten gefährdet sind.
2. Anhand der Ergebnisse Ihrer Bewertung sollten Sie die zehn wichtigsten Quellen sensibler MDM-Daten ermitteln, eine Strategie und einen Zeitplan zu ihrem Schutz festlegen und diese Strategie als Pilotprojekt für Ihren neuen Ansatz zur Erhöhung der Datensicherheit und des Datenschutzes umsetzen.
3. Definieren und dokumentieren Sie die Compliance-Richtlinien und die wichtigsten Stakeholder Ihres Unternehmens, die für Compliance mit gesetzlichen Vorschriften zuständig sind, und leiten Sie diese Informationen an alle Mitarbeiter weiter. Erstellen Sie einen strategischen Plan für das aktuelle Jahr und darüber hinaus.

Weitere Informationen

Die nachstehenden Publikationen und Videos enthalten weitere Informationen über Sicherheitsrisiken, denen sensible Daten ausgesetzt sind, sowie Faktoren, die beim Datenschutz zu berücksichtigen sind:

Informatica Data Privacy Management
Informatica Master Data Management – Customer 360
White Paper: Intelligenter Datenschutz
Bloor Research: Discovering Sensitive Data

Local Headquarters Ingersheimer Str. 10, 70499 Stuttgart Tel: +49 (0) 711 139 84-0 Gebührenfrei in den USA: 1.800.653.3871

IN09_0520_03409