Informatica

Lösungsübersicht

Fallstudie: Verhaltens-Analytics für Enterprise SaaS

Hauptvorteile

- Bereitstellung von Geschäftsprozessen mit schnellem und agilem Zugriffsmanagement
- Zuverlässige Nachverfolgung, wer wie auf sensible Daten zugreift
- Beseitigung der Ungewissheit hinsichtlich Gefährdungen durch interne Mitarbeiter und den Missbrauch von Zugangsdaten
- Bündelung von Reaktions- und Governance-Bemühungen, um auf Bedrohungen zu reagieren

Höhere Agilität und Geschwindigkeit für mehr Sicherheit

In der heutigen, wettbewerbsintensiven Unternehmenslandschaft stellen Geschwindigkeit, Agilität, Verfügbarkeit von Informationen und zuverlässige Daten für die schnelle Entscheidungsfindung wichtige Wettbewerbsvorteile dar, um sich von der Konkurrenz abzusetzen. Das traditionelle Sicherheitsmodell konzentriert sich auf die Implementierung sicherer Systeme, die Geschäftsanforderungen gerecht werden. Doch die immense Nachfrage nach Produkten direkt nach der Markteinführung führt dazu, dass selbst agile Sicherheitsteams Probleme haben, schnell genug zu agieren, und erzeugt Spannungen zwischen Sicherheits- und Betriebsteams.

Wie kann ein Sicherheitsteam mit geschäftlichen Änderungen Schritt halten und gleichzeitig dem Grundsatz der geringsten Rechte und dem Ziel von RBAC (Role-based Access Control) gerecht werden?

Informatica Secure@Source umfasst die Funktion „User Behavioral Analytics“ (UBA). So können Compliance-Modelle, die schon seit längerer Zeit von IT-Administratoren genutzt werden, unternehmensweit angewendet werden, so dass Dateneigentümer neue Erkenntnisse erhalten und genau wissen, wie und von wem ihre Daten verwendet werden. In Kombination mit Warnmeldungen und kurzen Reaktionszeiten können Datenverwalter und -eigentümer mithilfe von UBA das Risiko verringern, das durch die missbräuchliche Verwendung von Nutzerdaten und -rechten entsteht.

UBA nutzt Modelle, mit denen Audit- und Compliance-Teams vertraut sind, so dass selbst stark regulierte Umgebungen von einem schnellen Datenzugriff profitieren, ohne dass die Sicherheit beeinträchtigt wird.

Präzise Berechnung des Risikos, das durch unbefugte Nutzer besteht

Heutige Situation und neue Chancen

Wenn geschäftliche Veränderungen sehr schnell eintreten, können Bedenken zu Datensicherheit und -zugriff dazu führen, dass Änderungen nur langsam umgesetzt werden und Absatzchancen verloren gehen. Das kann dazu führen, dass Unternehmen Behelfslösungen nutzen und bestimmte Datenverwaltungsaufgaben und Analytics außerhalb des primären Schutzsystems vorgenommen werden.

Das führt zu einer Vielzahl an separaten Zugriffsbeschränkungen, die sich nur schwer verwalten lassen. Zudem ist es nicht ermöglichen, festzustellen, wer Zugriff auf welche Datensätze hat, und es ist nicht möglich, eine missbräuchliche Verwendung zu erkennen. Um Schutzmechanismen zu verbessern, ohne den laufenden Betrieb zu unterbrechen, müssen Unternehmen wissen, wie Geschäftsprozesse Daten nutzen und bereitstellen.

Dazu müssen verschiedene geschäftliche Anforderungen berücksichtigt werden. Geschwindigkeit und Agilität, gesetzliche Vorgaben für den Datenzugriff und Compliance-Vorgaben erfordern Funktionen, die nicht nur kontrollieren, auf welche Daten Nutzer Zugriff haben, sondern auch, wie sie diese Daten verwenden.

Informationen zu Informatica

Die digitale Transformation verändert unsere Welt. Als „Leader“ im Bereich Enterprise Cloud Data Management unterstützen wir Sie dabei, diese Transformation sinnvoll zu meistern. Wir ermöglichen es Ihnen, agiler zu werden, neue Wachstumsmöglichkeiten zu nutzen und Innovationen voranzutreiben. Wir laden Sie ein, das gesamte Angebot von Informatica zu erkunden – und das Potenzial der Daten zu nutzen um Ihre nächste intelligente Innovation auf den Weg zu bringen. Nicht nur einmal, sondern immer wieder.

Ansatz und Lösung

Unserer Erfahrung nach stellt UBA sicheren Datenzugriff bereit – ohne Einbußen bei Geschwindigkeit und Flexibilität. Bei internen Tests haben wir zunächst einige wichtige Geschäftsprozesse untersucht und den Weg der Datensätze verfolgt, von der zuverlässigen Quelle bis hin zu Analytics-Systemen und dem Reporting Stack. Durch die Analyse der Aktivitäten in der gesamten Datendomäne anstatt in nur einer Anwendung erhalten wir mehr Kontext zu den Aktivitäten der untersuchten Datensätze und wissen genau, wofür die Daten verwendet werden. Wir haben die Arten des Benutzerzugriffs nicht im Voraus festgelegt. Stattdessen haben wir die Aktivitäten von Nutzern überwacht und Funktionen zur Erkennung von Abweichungen und Reporting-Funktionen genutzt, um zuverlässige Ergebnisse zu erlangen.

Erkennung und Warnmeldungen alleine reichen nicht aus, um das Risiko zu senken. Es ist zwingend erforderlich, dass Nutzer, Dateneigentümer und Führungskräfte schnell auf Warnmeldungen reagieren. Daher sollte die Unterstützung von Dateneigentümern und Teamleitern bereits frühzeitig sichergestellt werden. Sie müssen die Verantwortung für das Risiko übernehmen, das durch ihren Datenzugriff entsteht. Dieses (mögliche) Risiko lässt sich am besten von der Datenperspektive her veranschaulichen. In den meisten Fällen haben Dateneigentümer und Führungskräfte nicht problemlos Einblick in Datenzugriff und Nutzungsmuster. Wenn Nutzer, Führungskräfte und Dateneigentümer einander Feedback geben, werden Nutzungsmuster und angemessene Verhaltensweisen gefestigt, so dass verantwortungsvolle Muster eingeführt werden können.

Es gibt zahlreiche Ähnlichkeiten zwischen diesem Ansatz und dem „Break-Glass-Zugriffsmodell“, das Administratoren sensibler Systeme normalerweise verwenden, um Zugriffsbeschränkungen bei Wartung und Fehlerbehebung zu umgehen. Der Administrator hat die entsprechenden Rechte, um die jeweilige Rolle auszuführen. Der Zugriff löst eine Überprüfung aus, um sicherzustellen, dass alle Aktionen autorisiert waren. Mithilfe von Machine Learning kann dieses Modell für das gesamte Unternehmen skaliert werden und wird von Auditoren als angemessen angesehen.

Ein erfolgreiches Programm sollte sich zunächst auf die Optimierung eines aktionsorientierten Reaktionsmodells konzentrieren, um auf Benutzerverhalten und Abweichungen zu reagieren. Danach sollte das Programm auf wichtige Geschäftsprozesse erweitert werden, für die Geschwindigkeit/Agilität wichtig sind bzw. die die Ziele des Unternehmens stark gefährden.

Schlussfolgerungen

Die Machine-Learning-Funktionen von Secure@Source bieten eine Zuverlässigkeit, die durch eine manuelle Überprüfung nicht erreicht werden kann. Dadurch sind die Zuweisung von Zugriffsberechtigungen und Datenverwendung besser aufeinander abgestimmt.

UBA lässt sich problemlos in Dateneigentümer-Modelle integrieren, um Dateneigentümer zu ermutigen, ihre Daten zu verwalten und zu schützen. Durch Sensibilisierungsprogramme, Schulungen und Prozess-Sanierung lassen sich Prozesse mithilfe von UBA verbessern und Änderungen umsetzen, damit das Unternehmen seinen Compliance-Zielen während des schnellen Wachstums stets gerecht wird.

Da UBA nicht an eine spezifische Anwendung oder Plattform gebunden ist, kann die Funktion anwendungsübergreifend genutzt werden. So kann ein ganzes Daten-Ökosystem geschützt werden, anstatt sich nur auf das Quellsystem zu konzentrieren, wodurch Reporting-Systeme außen vor bleiben.

Informatica Secure@Source UBA unterstützt die Geschäftsgeschwindigkeit und Agilität sowie auch Sicherheits- und Compliance-Ziele, indem Dateneigentümer und Führungskräfte in den Reaktionsprozess einbezogen werden.

Informatica

Informatica GmbH, Ingersheimer Str. 10, 70499 Stuttgart Tel.: +49 (0) 711 139 84-0 Fax: +49 (0) 711 139 84-600
Gebührenfrei in den USA: +1 800 653 3871
informatica.com/de linkedin.com/company/informatica twitter.com/Informatica

IN17_0617_3339