ForgeRock®

Whitepaper

Maximieren Sie den Wert Ihrer Identitätslösung mit KI-gestützten Identitätsanalysen

Einführung

Die Bedrohung der Datensicherheit von außen war nie größer. Umfang, Anzahl und Häufigkeit der Datenschutzverletzungen nehmen von Jahr zu Jahr zu. Auch die Zahl der Identitäten und Aktivitäten, die einen Zugriff erfordern, steigt rapide, ebenso wie der Umfang an Telearbeit. Dadurch wächst auch das Ausmaß der Bedrohungen von innen. Diese Ausweitung der Bedrohungslage wird durch Faktoren wie neue Identitätstypen (u. a. das Internet der Dinge (IoT), Operative Technologien (OT), sowie mobile Zugriffe) und den Übergang zu Cloud- und Hybrid-basierten Anwendungen noch verstärkt.

Mit der zunehmenden Bedrohung durch externe und interne Cyberrisiken kommt auch dem Identitätsmanagement eine immer größere Bedeutung zu, mit dem Ziel, Identitäten und Zugriffsrechte stärker abzusichern. Auch die Regulierungs- und Compliance-Landschaft wird demzufolge zunehmend komplex und strikt, was sich in der Einführung einer Vielzahl neuer Vorschriften und Richtlinien wie dem Sarbanes-Oxley Act (SOX), dem Health Insurance Portability and Accountability Act (HIPAA), der Europäischen Datenschutz-Grundverordnung (DSGVO) oder auch dem Federal Information Security Management Act (FISMA) zeigt. Bestehende IAM-Systeme und IGA-Lösungen (eine Unterkategorie der IAM-Systeme) sind den zunehmenden Herausforderungen und Anforderungen in diesem Umfang nicht gewachsen.

Im gleichen Maße, wie die externen und internen Bedrohungen und die Anzahl der Identitäten zunehmen, entwickelt sich auch der Bereich der Identitätsanalysen weiter, um die Herausforderungen zu meistern. Eine Identitätsanalyselösung, die künstliche Intelligenz (KI) und maschinelles Lernen (ML) nutzt, ermöglicht es Unternehmen, große Datenmengen sowie eine Vielzahl von Aktivitäten schnell zu analysieren.

KI-gestützte Analysen erlauben es, Zugriffsmuster von Nutzern mit niedrigem, mittlerem und hohem Risiko im gesamten Unternehmen zu erkennen. Darüber hinaus können sie sichere und risikoarme Entscheidungen automatisieren und schaffen so Raum für Risiko- und Sicherheitsteams, um nuancierte risikobehaftete Entschlüsse zu fassen. So lassen sich Ressourcen maximal ausschöpfen sowie Zugriffs- und Sicherheitsfehler reduzieren. Durch die Überlagerung und Integration von Identitätsanalysen in bestehende Identitätsmanagement- und Governance-Lösungen können Unternehmen Effizienz und Wert ihrer IAM- und IGA-Investitionen drastisch steigern.

In diesem Whitepaper werden die Entwicklungen im Bereich externer und interner Cyberbedrohungen sowie die Defizite herkömmlicher IAM- und IGA-Prozesse und -Lösungen diskutiert. Darüber hinaus wird beschrieben, wie ForgeRocks KI-gestützte Autonomous-Identity-Lösung in Echtzeit die kontinuierliche Sichtbarkeit, Kontrolle und Korrektur von Zugriffsrechten im Unternehmen gewährleistet.

Was ist künstliche Intelligenz?

Künstliche Intelligenz oder KI ist ein Gebiet im Bereich Computerwissenschaften, das sich der Lösung kognitiver Probleme widmet, die für gewöhnlich mit menschlicher Intelligenz in Verbindung gebracht werden, wie Lernen, Problemlösung und Mustererkennung. KI-Systeme treffen Entscheidungen, die normalerweise menschliches Wissen oder Fachkenntnisse voraussetzen. Diese Entscheidungen haben drei Dinge gemeinsam: Absicht, Intelligenz und Anpassungsfähigkeit.[1]

Was ist maschinelles Lernen?

Maschinelles Lernen ist eine von mehreren Methoden, die im Bereich der künstlichen Intelligenz eingesetzt wird. Es beschreibt den Prozess, bei dem einem Computersystem beigebracht wird, aufgrund eingespeister Daten präzise Vorhersagen zu treffen. Der Hauptunterschied zu herkömmlicher Computersoftware besteht darin, dass kein von einem menschlichen Entwickler geschriebener Code zur Anleitung des Systems verwendet wird. Ein Modell für maschinelles Lernen wird anhand einer großen Datenmenge mit oder ohne Aufsicht trainiert. Beim beaufsichtigten Lernen wird das System großen Mengen vorklassifizierter Daten ausgesetzt, während das unbeaufsichtigte oder nur zum Teil beaufsichtigte Lernen Algorithmen damit beauftragt, Datenmuster ohne menschliche Unterstützung oder Feedback zu identifizieren.[2]

Identitätsbedrohungen nehmen zu

Dem 2020 ForgeRock Consumer Identity Breach Report, zufolge haben Anzahl, Umfang und Häufigkeit von Datenschutzverletzungen, kompromittierten Daten und geschäftlichen Ziele während der letzten Jahre exponentiell zugenommen. Parallel dazu sind auch Aufwand und Kosten zum Schutz der Unternehmen vor diesen Bedrohungen angestiegen.

Noch bis vor Kurzem wäre die Nachricht, dass ein paar Hunderttausend Nutzer Opfer einer Datenpanne geworden sind, eine Schlagzeile wert gewesen. Mittlerweile sind im Falle einer Datenpanne häufig Millionen oder sogar Milliarden von Nutzern betroffen.

- Erst letztes Jahr landeten die Daten von 540 Millionen Facebook-Nutzern ungeschützt auf den Cloud-Servern von Amazon.[3]
- Beim US-amerikanischen Immobiliendienstleister First American Financial Corp waren die Daten von 885 Millionen Verträgen frei im Netz verfügbar. Diese Daten beinhalteten auch personenbezogene Daten wie Banktransaktionen und Sozialversicherungsnummern.[4]
- Yahoo bestätigte, dass rund drei Milliarden Nutzer bisher von Datenschutzverletzungen betroffen waren – dreimal mehr als ursprünglich angenommen. Das machte den Vorfall zum größten Datenskandal der Geschichte.[5]

Mit dem Ausmaß dieser Datenpannen steigen auch die Kosten für die Unternehmen.

- 2019 kostete eine Datenpanne in den Vereinigten Staaten ein Unternehmen im Schnitt 8,19 Millionen US-Dollar, ein Anstieg von 112 Prozent im Vergleich zu 2018.[6]
- Die Gesamtkosten aufgrund von Datenpannen in den Vereinigten Staaten beliefen sich 2019 auf über 1,2 Billionen US-Dollar; das ist ein Anstieg von 83 Prozent gegenüber 2018.[7]
- Der Technologiesektor verzeichnete 2019 dabei die höchsten Kosten aufgrund von Datenpannen: insgesamt 250 Milliarden US-Dollar nur in den Vereinigten Staaten.[8]

Die Daten zeigen klar, dass Ausmaß und Kosten externer Bedrohungen auf alarmierende Weise zunehmen.

Die interne Bedrohungslandschaft weitet sich aus

Die interne Bedrohungslandschaft weitet sich fast genauso schnell aus wie die Anzahl der externen Bedrohungen. Die Zahl der Identitäten und Aktivitäten, die von Unternehmen verwaltet und geschützt werden müssen, ist auf unglaubliche 3,2 Milliarden[9] Identitäten weltweit angestiegen. Es sind neue Identitätstypen hinzugekommen wie Verbraucher, IoT, OT und mobile Identitäten. Auch neue Geschäftsfaktoren spielen eine immer wichtigere Rolle wie die Forderung nach geschäftlicher Kontinuität und Resilienz, eine weit verstreute Belegschaft sowie zunehmende Telearbeit. Gleichzeitig werden Cloud-Anwendungen und Cloud-Anbieter in Geschäftseinheiten eingebunden. Die Folge: unvorhergesehene Abhängigkeiten und Schwachstellen.

All diese Faktoren tragen dazu bei, das Risiko unbeabsichtigter Datenschutzverletzungen zu erhöhen. Geschätzte 62 Prozent[10] aller Datenschutzverletzungen, die nicht auf Fehler, Missbrauch oder physische Aktionen zurückzuführen sind, wurden durch gestohlene Benutzerdaten, Brute-Force- oder Phishing-Angriffe verursacht. Darüber hinaus stellen Bedrohungen wie beispielsweise die Exfiltration von Mitarbeiterdaten, Datendiebstahl, Phishing-Angriffe, der unbefugte Zugriff durch Mitarbeiter sowie Spionage weitere Sicherheitsherausforderungen dar.

Die zunehmende Abhängigkeit von multiplen Cloud-Plattform-Anbietern wie Amazon Web Services (AWS), Google Cloud Services (GCS) und Microsoft Azure hat ebenfalls Schwachstellen zur Folge. Die durch die Implementierung von Authentifizierungsmechanismen, Zugriffskontrollen und Benutzermanagement über Cloud-Anbieter hinweg entstehenden Vernetzungen können leicht dazu führen, dass Dinge übersehen werden. So kann es passieren, dass ein Team, das mehrere Anbieter verwaltet, vielleicht vergisst, die voreingestellte Administratorkennung und das Passwort für eine oder mehrere Cloud-Umgebungen zu ändern.

Das ist besonders besorgniserregend, wenn man sich Statistiken ansieht, die zeigen, dass viele Unternehmen ihren Mitarbeitern zu umfangreiche Berechtigungen für den Zugriff auf Anwendungen, Dateien und Verzeichnisse gewähren.

- In einer im Jahr 2019 durchgeführten Umfrage fand das Datensicherheitsunternehmen Varonis heraus, dass jeder Mitarbeiter im Durchschnitt Zugriff auf 17 Millionen Dateien und 1,21 Millionen Verzeichnisse hat.[11]
- In der gleichen Umfrage fanden 58 Prozent der Unternehmen mehr als 1.000 Verzeichnisse mit den gleichen Berechtigungen.[12]
- Im Jahr 2019 stellte unbefugter Zugriff mit 40 Prozent die häufigste Form der Datenschutzverletzung dar, im Vergleich zu 34 Prozent im Jahr 2018.[13]

Dieser Anstieg zeigt deutlich, dass Unternehmen eine ausgefeiltere Identitätslösung einsetzen müssen, wenn sie Kriminelle vom Zugriff auf sensible Daten abhalten wollen.

Die Kosten von Datenschutzverletzungen

Aufgrund der Zunahme interner und externer Schwachstellen und Angriffe wurde die lange Liste bereits bestehender Vorschriften wie SOX, HIPAA, DSGVO und FISMA um neue Compliance-Richtlinien wie beispielsweise den California Consumer Privacy Act (CCPA) ergänzt, um sicherzustellen, dass Unternehmen ihre Nutzerdaten schützen. Diese wachsende Anzahl an Vorschriften hat zur Folge, dass die aufgrund von Datenschutzverletzungen anfallenden behördlichen Kosten und Gebühren ebenfalls gestiegen sind, ebenso wie die Anzahl quantifizierbarer Beispiele. Bis heute wurden beispielsweise 192 Millionen US-Dollar an Gebühren für DSGVO-Verstöße erhoben[14] – mit der höchsten Einzelstrafe in Höhe von 63 Millionen US-Dollar im Jahr 2019 gegen Google Frankreich. Deshalb sind IAM- und speziell IGA-Programme in unseren heutigen, dynamischen Unternehmen wichtiger denn je. Nimmt man dazu noch die explosionsartige Zunahme an digitalen Identitäten sowie die wachsende Anzahl Cloud-basierter Anwendungen und rechtlicher Vorschriften, kann man sich leicht vorstellen, dass IAM-Altsysteme dem Druck nicht mehr gewachsen sind.

Herkömmliche Identitätsmanagementlösungen sind nicht ausreichend

Die meisten Unternehmen nutzen herkömmliche IAM- und IGA-Lösungen für die Verwaltung der Zugriffsrechte, die Gewährleistung von Compliance und den Schutz der Daten. Angesichts externer Sicherheitsbedrohungen und der geradezu explosiven Zunahme an digitalen Identitäten sind diese Lösungen nicht länger in der Lage, eine umfassende, integrierte Sicht der Daten innerhalb des Unternehmens zu bieten. Auch kontextbezogene Analysen unterschiedlicher Identitätsdatenquellen sind damit nicht möglich.

Identitätssilos

Um die Risiken effektiv zu mindern und ihre Geschäftsdaten wirksam zu schützen, benötigen die Unternehmen absolute Transparenz sämtlicher Benutzerzugriffe. Egal, ob vor Ort eingesetzt oder Cloud-basiert: Ältere Identitätslösungen sind isoliert und können wahrscheinlich nicht alle Geschäftsanwendungen einbinden. Das Ergebnis ist eine fehlende unternehmensweite Transparenz von Benutzerzugriffen sowie ein mangelndes Bewusstsein für riskobehaftete Aktivitäten. Zudem ist es nicht möglich geeignete Zugriffsberechtigungen wie Berechtigungs- und Rollenzuweisungen zu empfehlen. Ohne kontextbezogene Perspektive verfügen die Unternehmen am Ende nur über eine isolierte Sicht auf schnell wachsende Identitätspopulationen (z. B. Mitarbeiter, Auftragnehmer, Partner und Verbraucher). Dieses Problem wird noch verschärft, wenn die Informationen über lokale und Cloud-basierte Umgebungen verteilt sind.

Dieser Kontext ist für die Einhaltung von Bestimmungen in einer komplexen Regulierungslandschaft besonders wichtig. Sicherheits- und Compliance-Teams müssen Identitäten und Zugriffe gemäß diesen Standards managen und steuern, aber ohne umfassende Transparenz gibt es keine Compliance. Eine wirklich effektive Lösung müsste absolut eindeutig darstellen, wer in welchem Kontext auf welche Anwendungen zugreifen darf, wie diese Zugriffsberechtigung zustandegekommen ist und wozu sie genutzt wird. Unternehmen müssen in der Lage sein, Risiken zu bewerten, um wichtige Geschäftsinformationen schützen zu können, und zwar einschließlich personenbezogener Daten, vertraulicher Informationen und geistigen Eigentums.

ForgeRock Autonomous Identity
Kundenerfolg

91 %

Ein multinationaler Finanzdienstleister identifizierte und automatisierte 91 % der Zugriffsberechtigungen für eine wichtige ERP-Anwendung.[15]

550.000

Ein großer US-amerikanischerGesundheitsdienstleister identifizierte 550.000 Zugriffsberechtigungen für die automatische Bereinigung.[15]

70 %

Ein multinationales Konsumgüterunternehmen verzeichnete eine Reduzierung der im Unternehmen erforderlichen Rollen um 70 %.[15]

Betriebliche Ineffizienzen

Angesichts zunehmender Risiken, Identitätsmengen und Compliance-Mandate müssen Unternehmen ein möglichst hohes Niveau an betrieblicher Effizienz erreichen. Daher muss die Automatisierung und Vereinfachung von Zugriffsanforderungen, Genehmigungen und Bearbeitung möglichst einheitlich erfolgen. Dies ist allerdings nur schwer umzusetzen, wenn Millionen von Zugriffsberechtigungen über verteilte Systeme, Anwendungen und Umgebungen verstreut sind.

Solche Ineffizienzen verringern die Produktivität und führen zu suboptimalen Geschäftsentscheidungen. Die meisten für die Genehmigung von Zugriffsrechten zuständigen Personen haben nur eine Wahl: nämlich Zugriffsanforderungen und Zertifizierungen ohne vollständig beschriebene Zugriffsrechte manuell zu genehmigen. So erhalten Benutzer völlig unbeabsichtigt zu umfassende bzw. falsche Zugriffsberechtigungen. Die schiere Menge an Anforderungen kann zwar überwältigend sein, aber ein solches Vorgehen widerspricht dem Sicherheitskonzept der minimalen Berechtigung, das viele Unternehmen umsetzen wollen.

Schwierige Integration

Angesichts der stetig wachsenden Zahl von Identitäten ist es eine echte Herausforderung, ältere Identitätslösungen mit mehreren Geschäftsanwendungen und Prozessen zu integrieren. Aus Architektursicht sind monolithische Altlösungen von Natur aus komplex. Das macht die Integration mit Unternehmensanwendungen zu einer gewaltigen, extrem ressourcenintensiven Aufgabe. Daher sind solche Identitätslösungen nur mit einer Untermenge von wichtigen Geschäftsanwendungen im gesamten Unternehmen integriert. Nimmt man die steigende Zahl an Sicherheits- und Compliance-Ressourcen hinzu, die für die Verwaltung dieser Altlösungen benötigt werden, führt dies zu einem massiven operativen Overhead. Und ohne die Fähigkeit, Identitätsdaten unternehmensweit über alle Anwendungen hinweg zu erfassen, ist es nahezu unmöglich, ein umfassendes Bild aller Identitätsrisiken zu erhalten.

Herkömmliche Identity-Governance-Lösungen sind nicht die Antwort

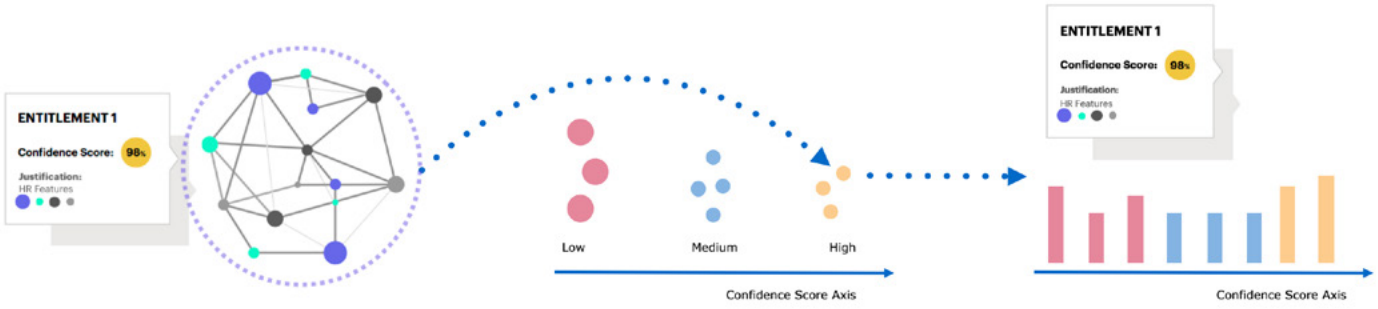
Angesichts zunehmender IT-Komplexität und der zunehmenden Risiken von Datenpannen und Datenschutzverletzungen werden IGA-Lösungen heute dringender als je zuvor benötigt. Sie sind nach wie vor ein wichtiger Bestandteil von umfassenden IAM-Unternehmensprogrammen, da sie zur Einhaltung von Compliance-Vorschriften beitragen, Vorteile hinsichtlich des Datenschutzes bieten und das User Lifecycle Management (ULM) im gesamten Unternehmen unterstützen. Allerdings reichen herkömmliche IGA-Ansätze nicht aus.

In der Regel ist nur eine begrenzte Anzahl von Unternehmensanwendungen in IGA-Lösungen integriert. Folglich mangelt es den meisten Organisationen an unternehmensweiter Transparenz hinsichtlich der Benutzerzugriffe und dem entsprechenden Bewusstsein für hohe Risiken. Zudem sind sie nicht in der Lage, geeignete Zugriffsprivilegien wie Berechtigungs- und Rollenzuweisungen zu empfehlen. Ein weiterer Grund dafür, dass IGA-Lösungen der ersten Generation immer weniger Nutzen bieten, liegt in der Komplexität der Implementierung und dem extremen Anpassungsbedarf, die umfangreiche Investitionen in Personal- und Budgetressourcen erforderlich machen. Diese Einschränkungen führen dazu, dass Unternehmen damit beginnen, ihre alten IGA-Konzepte durch modernere Lösungen zu ersetzen, die nur minimale Anpassungen erfordern und primär konfigurationsgesteuert sind. Unternehmen, die ihre digitale Transformation schnell bewältigen wollen, suchen nach Lösungen mit einer Abdeckung von 80 Prozent zu 20 Prozent der Kosten – etwas, das herkömmliche IGA-Lösungen nicht bieten können.

Ein moderner Ansatz: KI-gestützte Identitätsanalysen

Herkömmliche Identitätsmanagement- und Governance-Lösungen lassen sich mit KI-gestützten Identitätsanalysen ergänzen, um zugriffsbezogene Vorgänge zu skalieren und zu optimieren sowie unangemessene Zugriffsprivilegien zu bereinigen. ForgeRock Autonomous Identity bietet moderne, KI-gestützte Identitätsanalysen, mit denen herkömmliche Identitätslösungen ergänzt werden können. Damit ist es Unternehmen möglich, ihre Entscheidungsprozesse zu automatisieren und zu beschleunigen sowie vorhandene Investitionen zu maximieren.

So funktioniert's



1

Sämtliche Identitätsdaten wie Attribute, Berechtigungen und Rollen werden unternehmensweit erfasst, analysiert und modelliert.

2

Alle Confidence Scores werden berechnet und Benutzerzugriffsebenen mit niedrigem, mittlerem und hohem Risiko zugeordnet.

3

Jeder Confidence Score kann individuell geprüft und analysiert oder nach Zuordnung und Begründung analysiert werden.

Wie ForgeRocks Autonomous Identity mit den Herausforderungen von IAM-Altsystemen umgeht.

Herausforderungen bestehender IAM-Systeme	ForgeRock Autonomous Identity
Identitätssilos	Kontextbezogene, unternehmensweite Sichtbarkeit
Ältere IAM-Lösungen bieten eine isolierte Sicht auf Identitäten und die ihnen zugeordneten Zugriffsberechtigungen. Das liegt an der Vielzahl der unterschiedlichen in Unternehmen eingesetzten Identitäts-, Governance- und Infrastrukturplattformen. Jede Lösung enthält eine Untermenge an Identitäten (z. B. Mitarbeiter, Auftragnehmer und Partner), was blinde Flecken hinsichtlich der Benutzerzugriffsrisiken verursacht.	ForgeRock Autonomous Identity erfasst und analysiert Identitätsdaten von Identitäts-, Governance- und Infrastrukturplattformen, um alle Identitäten und ihre Zugriffe unternehmensweit transparent zu machen. So erhalten Sicherheits- und Compliance-Teams umfassende kontextbezogene Einblicke in alle Benutzerzugriffe mit geringem, mittlerem und hohem Risiko.

Herausforderungen bestehender IAM-Systeme	ForgeRock Autonomous Identity
Blinde Flecken bei Zugriffsberechtigungen	Bewusstsein für Zugriffsrisiken
Um sämtliche Identitäten zu erfassen und sichtbar zu machen, kaufen Unternehmen entweder Standard-IGA- und IAM-Lösungen oder entwickeln diese intern. Interne Lösungen bauen in der Regel auf Speicher-Repositorys auf, die strukturierte und unstrukturierte Daten in Datenseen speichern. Die Daten sind statisch und diese Lösungen bieten keine risikospezifischen Vorhersageerkenntnisse.	ForgeRock Autonomous Identity nutzt KI- und ML-Techniken, um proaktiv alle Identitätsdaten zu analysieren und Benutzerzugriffs- und Berechtigungsrisiken unternehmensweit im Kontext zu identifizieren. Die Lösung identifiziert schnell risikoreiche Nutzungszugriffe und Verletzungen des Zugriffs auf privilegierte und Root-Accounts und alarmiert die jeweiligen Sicherheits- und Compliance-Teams.
Herausforderungen bestehender IAM-Systeme	**ForgeRock Autonomous Identity**
Unangemessener Benutzerzugriff	Identifizierung von Zugriffsrechten
Der explosionsartige Anstieg digitaler Identitäten lässt die meisten Unternehmen in einer wahren Flut von Zugriffsanträgen, erschlichenen Berechtigungen und Zugriffszertifizierungen ertrinken. Um mit damit Schritt zu halten, genehmigen die Teams Zugriffsanforderungen und Zertifizierungen manuell en gros. Die daraus resultierenden zu umfangreichen Zugriffsrechte erhöhen die Risiken für das Unternehmen und verursachen zusätzliche Schwachstellen.	ForgeRock Autonomous Identity untersucht automatisch alle identitätsbezogenen Daten im gesamten Unternehmen und entlastet so die Sicherheits- und Compliance-Teams von manuellen Aufgaben. Durch die Analyse und schnelle Identifizierung angemessener Benutzerzugriffsrechte können Unternehmen proaktiv zu weit gehende Berechtigungen identifizieren und korrigieren, Abhilfemaßnahmen empfehlen und gegebenenfalls Berechtigungen automatisch widerrufen.
Herausforderungen bestehender IAM-Systeme	**ForgeRock Autonomous Identity**
Unangemessene Zugriffsberechtigungsmuster	Unternehmensweite Einblicke in Zugriffsrechte
Um zu entscheiden, ob ein Benutzer Zugriff auf ein System, eine Anwendung oder eine Umgebung mit einer herkömmlichen IAM- und IGA-Lösung haben soll, müssen Sicherheits- und Compliance-Teams große Mengen an Identitätsdaten manuell analysieren und überprüfen. Angesichts des exponentiellen Wachstums der Datenmenge ist es für Menschen einfach nicht möglich, unangemessene Zugriffsberechtigungsmuster über das gesamte Unternehmen hinweg effektiv zu identifizieren.	Durch die kontinuierliche Aufnahme neuer Identitätsdaten entwickelt ForgeRock Autonomous Identity sein ML-Modell weiter, um die dynamischen Veränderungen in einer Organisation zu verstehen. Dadurch ist es möglich, Ausreißer vorherzusagen und zu identifizieren, einschließlich unangemessener Zugriffsberechtigungsmuster. Dieser auf Datenintelligenz basierende Ansatz ermöglicht es Sicherheits- und Risikoteams, große Mengen von Identitätsdaten automatisch zu analysieren und abzubilden und so mit hohem Risiko behaftete und unbefugte Benutzerzugriffe im gesamten Unternehmen zu identifizieren.
Herausforderungen bestehender IAM-Systeme	**ForgeRock Autonomous Identity**
Manuelle Korrektur von Benutzerzugriffen	Automatische Korrektur von Benutzerzugriffen
Es ist extrem zeitaufwendig, Benutzerzugriffe in herkömmlichen IGA- und IAM-Lösungen manuell zu erstellen, zu überprüfen und zu genehmigen/zu widerrufen. Wenn unangemessene Benutzerzugriffe manuell identifiziert werden, müssen Sicherheits- und Compliance-Teams diese über mehrere Systeme, Anwendungen und Umgebungen hinweg manuell korrigieren – und zwar sowohl lokal als auch in der Cloud. Die Durchführung und Bestätigung erfordert viel Zeit, Mühe und Ressourcen und in der Zwischenzeit ist das Unternehmen anfällig für Angriffe.	ForgeRock Autonomous Identity ermöglicht die automatische Genehmigung und Zertifizierung von hoch sicherheitsrelevanten, risikoarmen Zugriffsanfragen sowie den automatischen Widerruf von veralteten Benutzerzugriffsrechten und das Löschen von Benutzern. Diese KI-gestützte Analyse senkt den Aufwand für operative Zugriffsanfragen und beschleunigt Zertifizierungskampagnen in der gesamten Organisation, ohne das Unternehmen unnötigen Risiken auszusetzen.

KI-gestützte Identitätsanalysen leicht gemacht – mit ForgeRock

Die Vorteile von ForgeRock Autonomous Identity

Kontextbezogene unternehmensweite Risikotransparenz

- Gefährdungslage von Unternehmen durch Benutzerzugriffe verstehen
- Kontextbezogene Kenntnis darüber, wer warum Zugriff auf was hat
- Kontinuierliche Identifizierung und Überwachung risikoreicher Zugriffe
- „Single Source of Truth“

Verbesserte betriebliche Effizienz

- Automatische Transparenz und Berichterstattung von Benutzerzugriffsrisiken
- Automatische KI-gestützte Analyse von Benutzerzugriffsrisiken
- Produktivitäts-verlagerungen, Konzentration auf und Erledigung von Aufgaben mit höherer Priorität
- Reduzierung manueller Genehmigungen und Zertifizierungen

Beschleunigte Entscheidungspro zesse

- Risikobasiertes Genehmigen / Widerrufen von Benutzerzugriffen durch Entscheider
- Maßnahmen-ergreifung auf Basis von Confidence Scores anstatt statischer Rollen und Berechtigungen
- Unmittelbare Entscheidungen auf Basis von Benutzerzugriffsdaten

Zukunftsfähig

- Beschleunigte Zugriffsberechtigungen für neue Mitarbeiter durch Empfehlungen auf Basis von Confidence Scores
- Schnellere Entscheidungen zum User Provisioning auf Basis einer höheren Vertrauensstufe
- Geringerer Zeitaufwand für Genehmiger und Zertifizierer durch automatische Genehmigung von als hochvertraulich eingestuften Zugriffsanforderungen und Zertifizierungen

Angesichts externer Cyber-Bedrohungen, die in einem noch nie dagewesenen Tempo zunehmen, und ständigen internen Herausforderungen müssen Sicherheits- und Risikoexperten intelligenter – und nicht härter – arbeiten, um ihr Unternehmen umfassend und wirksam zu schützen. Bestehende Identitäts- und Governance-Lösungen und -Prozesse müssen verbessert werden. Dies lässt sich durch den proaktiven Einsatz einer Lösung für KI-gestützte Identitätsanalysen erreichen.

ForgeRock Autonomous Identity ermöglicht es Ihnen, Identitätsanalysen in Ihre bestehenden IAM- und IGA-Lösungen zu integrieren. Die Lösung nutzt künstliche Intelligenz und maschinelles Lernen, um Informationen bereitzustellen, auf deren Basis Unternehmen Compliance-Standards zuverlässig einhalten können. Zudem können sie schnell und effizient das Sicherheitskonzept der minimalen Berechtigung umsetzen und kontinuierlich über die im Unternehmen geltenden Benutzerberechtigungen auf dem Laufenden bleiben. Die Maximierung Ihrer bestehenden IAM- und IGA-Investitionen mit ForgeRock Autonomous Identity sorgt unternehmensweit für kontextbezogene Risikotransparenz, verbessert die betriebliche Effizienz und gewährleistet, dass Ihre Sicherheitslage mit dem immer schnelleren Rhythmus der digitalen Welt Schritt halten kann.

Mehr zu ForgeRock Autonomous Identity

Besuchen Sie unsere Webseite, um weitere Informationen zu ForgeRock Autonomous Identity zu erhalten oder setzen Sie sich noch heute mit uns in Verbindung, um Ihre persönliche Reise ins Reich KI-gestützter Identitätsanalyse zu beginnen.

Endnoten

1 https://www.brookings.edu/research/what-is-artificial-intelligence/

2 https://www.zdnet.com/article/what-is-machine-learning-everything-you-need-to-know/

3 https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/

4 https://gizmodo.com/885-million-sensitive-records-leaked-online-bank-trans-1835016235

5 https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1

6 Die Schätzung der Kosten basiert auf der Anzahl der insgesamt festgestellten Datenschutzverletzungen und den Ergebnissen einer Studie des Ponemon Institute zu den Kosten einer Datenpanne in den USA („Cost of a Data Breach Report 2019“).

7 https://www.forgerock.com/resources/2020-consumer-identity-breach-report

8 ebd.

9 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

10 https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

11 https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

12 https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

13 https://www.forgerock.com/resources/2020-consumer-identity-breach-report

14 https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

15 ForgeRock Autonomous Identity Customer Success Report 2020