Sicherheit. Compliance.

Warum Zugriffsmanagement nicht ausreicht

SailPoint

Der rasante Übergang zur digitalen Welt erfordert tiefgreifende Veränderungen in der Art und Weise, wie Unternehmen ihre Belegschaft verwalten und vor allem, wie sie den Zugriff auf kritische Anwendungen und Daten bereitstellen und steuern. Diese Belegschaft besteht nicht mehr nur aus menschlichen Anwendern – Mitarbeitern, externen Dienstleistern und Lieferanten – sondern auch aus Bots oder Servicekonten, die jeweils ihre eigenen Zugriffsanforderungen, Einschränkungen und Standorte benötigen. Außerdem wird auf Daten und Anwendungen, die über Cloud-, On-Premise- und hybride Infrastrukturen verteilt sind, von überall aus und über eine Vielzahl von Geräten zugegriffen.

Heutzutage verlassen sich viele Unternehmen auf Identity-Tools, um den Zugriff für Mitarbeiter schnell zu authentifizieren und zu föderieren. Auch wenn diese Tools oft grundlegende Lifecycle-Management-Funktionen bieten, um Mitarbeitern rund um die Uhr Zugriff zu ermöglichen, fehlt es ihnen an den erforderlichen Sicherheitszugriffskontrollen und -richtlinien, um effektiv zu wissen, wer auf was zugreifen kann, und – noch wichtiger – um den Zugriff darauf basierend zu gewähren, wer auf was zugreifen sollte. Diese Unternehmen halten unwissentlich ihr Risiko hoch, indem sie Zugriffsrechte ohne Governance-Überwachung und -Durchsetzung gewähren.

Diese Zugriffsrisiken können nur durch Identity Security gelöst werden, die angemessene Zugriffskontrollen einführt, um das Risiko toxischer Zugriffskombinationen zu mindern, die den Mitarbeiterzugriff bei sich ändernden Arbeitsrollen/-funktionen aktualisiert und die Zugriffsrisiken kontinuierlich überwacht.

Verhindern Sie blinde Flecken bei Zugriffsverwaltung und Überprovisionierung

Durch die Implementierung eines durchgängigen Identity-Programms, das Funktionen für die Zugriffsverwaltung wie SSO und MFA mit dem Lifecycle Management und der Governance von Identity Security integriert, können Unternehmen ihre Umgebung sichern und gleichzeitig von der Effizienz einer integrierten Strategie profitieren.

Dies können Sie mit einem Bürogebäude und seiner Sicherheitsausstattung vergleichen. Um das Gebäude betreten zu können, müssen Sie einen Ausweis vorlegen, der beweist, dass Sie derjenige sind, für den Sie sich ausgeben. Dies ist die Authentifizierung bei der Zugriffsverwaltung. Auch wenn Ihnen der Zutritt gewährt wird, muss kontrolliert werden, wohin Sie gehen können und worauf Sie Zugriff haben (welche Etagen, welche Räume, welche Systeme), da Mitarbeiter, Gäste, externe Dienstleister und Lieferanten alle unterschiedliche Zugriffsebenen benötigen. Hier kommt Identity Security ins Spiel: Sie führt Richtlinien ein, um sämtlichen Nutzerzugriff ordnungsgemäß zu verwalten, damit jeder Mitarbeiter genau den Zugriff hat, den er für seine Arbeit benötigt. Nicht mehr und nicht weniger. Ohne diese Vorkehrungen fühlen sich Unternehmen in falscher Sicherheit und sind möglicherweise ungeschützt.

Ein Lifecycle-Management-Tool, das über keine Identity Security Kontrollmechanismen verfügt, kann schnell zu einer Überprovisionierung (Personen erhalten Zugriff, die diesen nicht haben sollten) sowie zu Compliance-Problemen (Kritische Daten werden nicht geschützt) führen. Die größte Gefahr besteht jedoch darin, was passieren kann, wenn Konten kompromittiert werden oder das Ziel von internen oder externen Bedrohungen sind: katastrophale Datenschutzverletzungen und kostspielige Compliance-Verstöße.

Da 94 % aller Verstöße mit Identity in Verbindung stehen, ist es entscheidend, dass der Zugriff auf alle Ihre Unternehmensressourcen gesichert, überwacht und gesteuert wird.[1]

Mit der Power von SailPoint Identity Security können Unternehmen umfassendes End-to-End-Identity-Management ermöglichen, indem sie das Zugriffsmanagement mit KI-gesteuerter Identity Security vereinen, um den Zugriff auf alle Anwendungen und Daten im gesamten Unternehmen effektiv zu authentifizieren, zu provisionieren und zu steuern.

Das Ergebnis ist ein Identity-bewusstes Unternehmen, das effizienter, sicherer und richtlinienkonform ist.

Eine Identity-bewusste Infrastruktur ist essentiell für moderne Unternehmen, die Sicherheitsrisiken und Compliance-Anforderungen proaktiv angehen und gleichzeitig die strategischen Ziele des Unternehmens effektiv erfüllen müssen.

Mit der SailPoint Identity Plattform und der Power von KI und maschinellem Lernen (ML) profitieren Unternehmen von unübertroffener Transparenz und Intelligenz, während sie gleichzeitig die Verwaltung aller Benutzeridentitäten, Berechtigungen, Systeme, Daten und Cloud-Dienste automatisieren und beschleunigen können – einschließlich der Fähigkeit, Cloud-IaaS-Umgebungen wie AWS und Azure zu verwalten und zu sichern.

[1]2020 IDSA Report: Identity Security a Work in Progress

Die Power von Identity Security

Identity Security schützt Unternehmen vor dem inhärenten Risiko, das mit der Bereitstellung von Technologiezugang für die moderne, vielfältige Remote-Belegschaft einhergeht. Dies sind einige der Hauptvorteile von SailPoint Identity Security:

- Rundumansicht aller Benutzertypen und ihres Zugriffs, einschließlich aller Berechtigungen, Attribute und Rollen.
- Automatische Provisionierung, Anpassung und Beendigung von Zugriff, wenn Mitarbeiter dem Unternehmen beitreten, dieses verlassen oder die Rolle wechseln.
- Identifizierung riskanten Verhaltens und umgehende Behebung dank KI-gestützter Einblicke und Empfehlungen, damit Sie wissen, wann der Zugriff sicher erteilt werden kann und wann nicht.
- Durchsetzung von Richtlinien für den Benutzerzugriff, beispielsweise für die Aufgabentrennung, und Einrichtung durchgängiger Kontrollen zur Vermeidung von Zugriffsverletzungen oder übermäßig berechtigter Benutzer.
- Nutzungsverfolgung und kontinuierliche Überwachung der Wirksamkeit der Zugriffskontrollen für Apps, Daten und Cloud, damit die Berechtigungen richtlinienkonform sind.
- Reduzierung der IT-Kosten und Eliminierung von Helpdesk-Anrufen durch die Automatisierung von Identity-Prozessen wie Onboarding, Passwortrücksetzungen und Berechtigungsanforderungen.
- Aufdeckung und Schutz sensibler Daten, einschließlich Cloud-Dateispeicher, sodass Benutzer über die richtige Zugriffsebene verfügen.
- Anpassung der Zugriffskontrollen und -richtlinien mit zunehmender Weiterentwicklung Ihres Unternehmens und Auftreten von Bedrohungen mithilfe adaptiver Governance.

Stellen Sie Ihre Identity Security Strategie auf

Unternehmen müssen das Gesamtbild im Auge behalten und einen strategischeren Ansatz bei der Verwaltung ihrer Identitäten und beim Aufbau von Cyber-Resilienz verfolgen. Ein Identity-Programm umfasst sehr viel mehr als nur den Zugriff, der die Spitze des Eisbergs bildet. Unter der Oberfläche befindet sich der Identity-Kontext, der durch ein Identity Security Programm gewonnen wird. Mit diesem reichhaltigen Kontext wird ein intelligenteres Identity Management ermöglicht, indem der Austausch mit anderen entscheidenden IT- und Sicherheitsressourcen im IT-Ökosystem gefördert wird. Bei einem intelligenten Identity-Ansatz erkennen Unternehmen schnell, dass dieser sehr viel mehr umfasst als nur die Steuerung und Provisionierung von Anwendungen, Lifecycle Management, Zertifizierung und Passwortverwaltung. Es handelt sich um das Verbindungsglied, das alle Ihre Sicherheits- und Compliance-Bemühungen miteinander vereint.

Wenn Sie diese Fragen bei der Planung Ihrer Identity-Strategie nicht beantworten können, kann Identity Security Abhilfe schaffen:

1. Verfügen Sie über die volle Transparenz und Kontrolle über alle Arten von Benutzern und alle Apps (sowohl On-Premise als auch in der Cloud), Dateien und Cloud-Plattformen innerhalb Ihres Unternehmens?
2. Erhalten Ihre Mitarbeiter nur den richtigen Zugriff auf die richtigen Ressourcen zur richtigen Zeit? Ist dieser Vorgang automatisiert?
3. Können Sie Ihre IT-Abteilung entlasten, indem Sie repetitive, risikoarme Aufgaben identifizieren, die dank KI-gestützter Empfehlungen auf sichere Weise automatisiert werden können?
4. Wissen Sie, was Ihre Benutzer mit dem Zugriff auf Ihre Unternehmensressourcen anstellen?
5. Können Sie den Zugriff automatisch anpassen oder beenden, wenn sich die Rollen Ihrer Benutzer ändern?
6. Können Sie automatisch einen Bericht für Ihre Auditoren erstellen und kontinuierliche Compliance sicherstellen?
7. Können Sie verdächtige Aktivitäten melden und die zuständigen Administratoren alarmieren?

Ermöglichen Sie Nutzerzugriff und schützen Sie Ihr Unternehmen überall mit Identity Security für Cloud-Unternehmen von SailPoint.

Erfahren Sie mehr unter **www.sailpoint.com/platform**.

ÜBER SAILPOINT

SailPoint ist der führende Anbieter von Identitätslösungen für Unternehmen in der Cloud. Wir haben es uns zur Aufgabe gemacht, die Risiken auszuräumen, die mit der Bereitstellung von Benutzerzugriffen für eine vielfältige und verteilte Belegschaft einhergehen. Unsere Identitätslösungen schützen und unterstützen Tausende von Unternehmen weltweit. Sie vermitteln unseren Kunden hervorragende Übersicht über ihre gesamte digitale Belegschaft und sorgen dafür, dass jeder Mitarbeiter genau die Zugriffe hat, die er für seine Arbeit benötigt – nicht mehr und nicht weniger. Mit SailPoint als Grundlage der Unternehmenssicherheit können unsere Kunden sicheren Zugriff gewährleisten, ihre Assets bedarfsgerecht schützen und die Compliance-Vorgaben erfüllen.

EB1931-2106