okta

Governance für alle Identitäten: 5 Schritte zur Modernisierung Ihrer Identity Governance

Durch die aktuelle rasante KI-Einführung und den unkontrollierten Cloud-Wildwuchs wurde der klassische Netzwerkperimeter aufgeweicht, sodass Identity Governance zur zentralen Grundlage einer sicheren Umgebung wird. Diese Checkliste liefert Ihnen eine strategische Roadmap, mit der Sie den vorhandenen Schutz Ihrer Umgebung überprüfen und die Lücken zwischen menschlicher und nicht-menschlicher Sicherheit schließen. Wenn Unternehmen zentrale Aufgaben wie die anfängliche Bestandsaufnahme und die automatisierte Lebenszyklusverwaltung bewältigen, können sie Maßnahmen ergreifen und sicherstellen, dass alle Identitäten – seien es menschliche Benutzende, nicht-menschliche Identitäten oder KI-Agenten – erfasst, nach dem Least-Privilege-Prinzip verwaltet und kontinuierlich auf Risiken überwacht werden.

Bestandsaufnahme aller Identitäten

Die Etablierung einer zentralen Informationsquelle für Ihren Identity Security Fabric reduziert blinde Flecken, die durch Schatten-KI und nicht verwaltete Service-Accounts entstehen.

- ☐ Katalogisieren Sie alle Benutzenden, nicht-menschlichen Identitäten und KI-Agenten.
- ☐ Erfassen Sie sanktionierte und Schatten-Accounts sämtlicher Typen.
- ☐ Scannen Sie Agentenplattformen (z. B. AWS Bedrock, Vertex AI).
- ☐ Identifizieren Sie alle Identitäten (Mitarbeitende und nicht-menschliche) in Cloud-, On-Premise- und SaaS-Plattformen.
- ☐ Erkennen Sie verwaiste oder inaktive Accounts ohne aktive verantwortliche Person.
- ☐ Ordnen Sie jede Identität den Systemen und Daten zu, auf die sie zugreifen kann.

Zuweisung menschlicher verantwortlicher Personen

Wenn jede digitale Entität an eine verantwortliche Person gebunden ist, werden alle automatisierten Aktionen an einen klaren Geschäftskontext gebunden.

- ☐ Ordnen Sie jede Identität (menschliche Benutzende, nicht-menschliche Identitäten und KI-Agenten) einer verantwortlichen Person oder einem Team zu.
- ☐ Dokumentieren Sie den geschäftlichen Zweck für jede Identität.
- ☐ Stellen Sie sicher, dass die Verantwortung übertragen wird, wenn Mitarbeitende ihre Funktion wechseln oder das Unternehmen verlassen.
- ☐ Kennzeichnen und sperren Sie jede Identität ohne gültige, aktive verantwortliche Person.

Okta Identity Governance

Durchsetzung des Least-Privilege-Prinzips durch automatisierte Zugriffsüberprüfungen und Provisionierungen

okta

Anwendung des Least-Privilege-Prinzips

Durch die Implementierung eines ZSP-Modells (Zero-Standing Privilege) wird sichergestellt, dass der Zugriff nicht dauerhaft ist. Dies kann die Auswirkungen kompromittierter Anmeldedaten erheblich reduzieren.

- ☐ Gewähren Sie nur Zugriff auf das, was unbedingt erforderlich ist.
- ☐ Verwenden Sie Just-in-Time-Token (JIT) anstelle von langlebigen Standing Credentials.
- ☐ Beseitigen Sie festcodierte API-Keys und Static Credentials, die in Code oder Pipelines gespeichert sind.
- ☐ Stellen Sie sicher, dass der delegierte Zugriff und der Zugriff von Unteragenten enger gefasst ist als der Umfang der Sponsor-Identität.
- ☐ Erzwingen Sie die Funktionstrennung (Separation of Duties, SoD), indem Sie gefährliche Zugriffskombinationen identifizieren und beheben.

Standardisierung von Zugriffsprüfungen

Die Anwendung einheitlicher Zertifizierungsstandards für alle Identity-Typen bietet eine kontinuierliche Validierung, dass die Berechtigungen im Laufe der Zeit mit den tatsächlichen Geschäftsanforderungen übereinstimmen.

- ☐ Wenden Sie die gleichen Überprüfungs- und Zertifizierungsstandards auf Service-Accounts, Agenten und Mitarbeitende an.
- ☐ Führen Sie regelmäßige Rezertifizierungskampagnen für risikoreiche Benutzende und Agenten durch.
- ☐ Suchen Sie aktiv nach SoD-Verletzungen und widersprüchliche Berechtigungen für jede Identität unter Berücksichtigung der Berechtigungsbereiche.
- ☐ Sperren Sie Zugriffsrechte, die nicht mehr geschäftlich gerechtfertigt sind.
- ☐ Kennzeichnen Sie alle Berechtigungen, die über ihren ursprünglichen Umfang hinaus erweitert wurden.
- ☐ Dokumentieren und befristen Sie alle Ausnahmen, einschließlich genehmigter SoD-Überschreibungen.

Automatisierung der Lebenszyklusverwaltung

Durch die Automatisierung des Identity-Lebenszyklus – vom ersten Tag bis zum Offboarding – kann die Sicherheit ohne manuelle Eingriffe mit der Geschwindigkeit des Unternehmens Schritt halten.

- ☐ Leiten Sie die gesamte Identity-Provisionierung über einen genehmigten Anfrage- und Workflow-Prozess.
- ☐ Deprovisionieren Sie automatisch Anmeldedaten, wenn ein Workflow, eine Aufgabe oder ein Arbeitsverhältnis endet.
- ☐ Legen Sie den Ablauf von Anmeldedaten in Abhängigkeit von Rolle oder Aufgabendauer fest.
- ☐ Widerrufen Sie den Agentenzugriff, wenn die zuständigen Mitarbeitenden das Unternehmen verlassen.
- ☐ Automatisieren Sie die Erkennung von ungenutzten oder verwaisten Accounts für jeden Identity-Typ.

Lifecycle Management

Automatisierung des Joiner-, Mover- und Leaver-Prozesses, um manuellen Aufwand zu eliminieren und Sicherheitslücken zu schließen

Maximierung der Governance-Strategie

Laden Sie unser E-Book für sicherheitsorientierte Governance herunter, das Ihnen hilft, Ihre Governance-Strategie zu modernisieren. Sie erfahren, wie Sie von isolierten, manuellen Prozessen zu automatisierter Resilienz für alle menschlichen Benutzenden, nicht-menschlichen Identitäten und KI-Agenten in Ihrem Ökosystem übergehen können.

Unabhängig davon, ob Sie die meisten dieser Anforderungen bereits erfüllt haben oder gerade erst mit der Bestandsaufnahme Ihrer Umgebung beginnen, bietet Okta Identity Governance die strategische Grundlage für die Modernisierung Ihrer Gesamtsicherheit.

Durch den Wechsel von manuellen, isolierten Prozessen zu einem einheitlichen Identity Security Fabric kann Ihr Unternehmen den gesamten Lebenszyklus für alle menschlichen Benutzenden, nicht-menschlichen Identitäten und KI-Agenten automatisieren.

Implementieren Sie statt statischer Berechtigungen ein Modell für kontinuierliche, automatisierte Resilienz, mit dem das Least-Privilege-Prinzip und „Just-in-Time“-Zugriff durchgesetzt wird, ohne Ihr Geschäft zu verlangsamen.

Mehr über Okta Identity Governance

Über Okta
Okta ist das weltweit führende Identity-Unternehmen. Wir schützen die Identität von KI-Agenten, Maschinen und menschlichen Benutzenden, damit unsere Kundinnen und Kunden sowie Partner jede Technologie sicher nutzen können. Unsere Lösungen unterstützen Unternehmen sowie Entwicklungsteams dabei, die Sicherheit und Effizienz zu steigern und die Ziele zu erreichen. Gleichzeitig werden Benutzende, Mitarbeitende sowie Partner zuverlässig geschützt. Weltweit führende Marken vertrauen bei Authentifizierung, Autorisierung und mehr auf Okta. Weitere Informationen finden Sie unter okta.com/de.