Microsoft Entra ID Governance

Zentrale Benutzer- und Rechteverwaltung in Cloud-Landschaften

Mit Microsoft Entra ID Governance lassen sich Benutzer und Zugriffsrechte in unterschiedlichen IT-Systemen zentral und benutzerfreundlich verwalten. Die Software unterstützt effiziente Abläufe durch umfangreiche Automatisierungs- und Self-Service-Funktionen und sorgt dank integriertem Reporting und Monitoring für die Einhaltung von Compliance- und Transparenzvorgaben.

Cloudbasierte Zugriffsverwaltung

Microsoft Entra ID Governance ist eine cloudbasierte Identitätsgovernancelösung. Sie bietet Möglichkeiten zur Steuerung des Identitätslebenszyklus, des Zugriffslebenszyklus und die Sicherung des privilegierten Zugriffs für die Verwaltung. Zu den Funktionen gehören unter anderem die Erstellung von Workflows zur automatischen Verwaltung von Berechtigungen, die Steuerung von App- und Ressourcenzugriffen anhand von Gruppenzugehörigkeiten und das Delegieren von Zugriffsentscheidungen an Unternehmensgruppen. Microsoft Entra ID Governance unterstützt sowohl lokale als auch cloudbasierte Anwendungen und eine Vielzahl an HR-Systemen, wie SAP SuccessFactors, workday und Microsoft Dynamics 365.

Für den Lebenszyklus von Identitäten

Das Zugriffs- und Berechtigungsmanagement in Unternehmen ist ein erheblicher Zeit- und Kostenfaktor, da die Implementierung einer Identitäts- und Zugriffsverwaltung sowie deren Wartung meist mit viel Aufwand verbunden ist. Hinzu kommt, dass angesichts der fortschreitenden technischen Entwicklung immer mehr unterschiedliche Betriebssysteme und Applikationen Einzug in die Unternehmen halten. Zudem wächst die Zahl der mobil arbeitenden Mitarbeiter mit den entsprechenden Endgeräten stetig. Mehr denn je sind Nutzer also darauf angewiesen, zielgerichtet wie auch remote auf ihre notwendigen Daten und Applikationen zugreifen zu können. Und zwar stets vor dem Hintergrund von geltenden Sicherheitsbestimmungen und Gesetzesvorgaben. Mittels einzelner „Insellösungen“ und manuellen Prozessen lässt sich dem auf Seiten der IT-Abteilung jedoch kaum noch Herr werden.

Für den Lebenszyklus von Zugriffen

Mit Microsoft Entra ID Governance können IT-Abteilungen festlegen, welche Zugriffsrechte Benutzer für verschiedene Ressourcen haben sollten und welche Kontrollen zur Durchsetzung erforderlich sind, z. B. Aufgabentrennung oder Zugriffsentzug bei Stellenwechsel. Die Microsoft Entra-ID verfügt über Connectors zu Hunderten von Cloud- und lokalen Anwendungen. Wenn ein Benutzer versucht, sich bei einer dieser Anwendungen anzumelden, erzwingt Microsoft Entra ID Richtlinien für bedingten Zugriff.

Zugriffsänderungen in Apps und Gruppen können basierend auf Attributänderungen automatisiert werden. Darüber hinaus kann die IT Zugriffsverwaltungsentscheidungen an Entscheidungsträger des Unternehmens delegieren. Mit der Berechtigungsverwaltung können Sie festlegen, wie Benutzer den Zugriff über Pakete von Gruppen- und Teammitgliedschaften, App-Rollen und SharePoint Online-Rollen hinweg beantragen, und Sie können Prüfungen der Aufgabentrennung bei Zugriffsanfragen durchsetzen. Außerdem können Organisationen steuern, welche Gastbenutzer Zugriff auf lokale Anwendungen haben.

Für den Lebenszyklus von Privilegien

Microsoft Entra Privileged Identity Management (PIM) bietet zusätzliche Steuerungen für den Schutz der Zugriffsrechte für Ressourcen in Microsoft Entra, Azure, anderen Microsoft Online Services und anderen Anwendungen zugeschnitten sind. Zusätzlich zur Multi-Faktor-Authentifizierung und zum bedingten Zugriff stehen Ihnen mit den Funktionen für Just-In-Time-Zugriff und Warnungen für Rollenänderungen von Microsoft Entra PIM umfassende Governancekontrollen zum Schützen der Ressourcen Ihrer Organisation (Verzeichnisrollen, Microsoft 365-Rollen, Azure-Ressourcenrollen und Gruppenmitgliedschaften) zur Verfügung. Wie bei anderen Formen des Zugriffs können Organisationen mithilfe von Zugriffsüberprüfungen eine periodische erneute Zertifizierung für alle Benutzer mit privilegierten Administratorrollen konfigurieren.

Produktmerkmale & Features

- Abdeckung aller wichtigen Bereiche von IAM in einer integrierten Cloudlösung
- Identity Lifecycle Management (z.B.: Onboarding / Wiedereinstellung / Kündigung / Langzeitkrank / Elternzeit / Rente und mehr)
- Integration in Sicherheits- und Risikoanalysen der Microsoft Entra ID und des Microsoft 365-Ökosystems
- Integrierte Unterstützung für dezentrale Identitäten
- Gateways für die Integration zurück in lokale Umgebungen

Ihr Nutzen auf einen Blick

- Verwaltung des Zugriffs auf lokale, cloudbasierte und hybride Ressourcen als öffentlicher, mandantenfähiger Cloud-Service
- Minimierung von Risiken durch beschränkten Zugang der Benutzer auf ausschließlich benötigte Anwendungen
- Einfache Umsetzung von Compliance-Anforderungen
- Hohe Flexibilität durch die Möglichkeit zur Integration von Nicht-SAP-Systemen
- Zahlreiche Konnektoren für andere Systeme
- Hohe Systemkompatibilität, die eine Erweiterung bestehender Infrastrukturen ermöglicht

"Das Management von Zugriffen, Identitäten und Privilegien beansprucht zu viele personelle Kapazitäten, insbesondere in der IT-Abteilung. Microsoft Entra ID Governance vereinfacht diese Herausforderung, indem die Verwaltung zentralisiert und die Prozesse automatisiert werden. Dadurch wird die Komplexität

des Identitäts- und Zugriffsmanagements spürbar reduziert. Zudem wird sichergestellt, dass regelkonform genau die Zugriffsrechte vergeben werden, die die Mitarbeitenden tatsächlich benötigen – und das während des gesamten Lifecycles von Identitäten, Zugriffen und Privilegien."

Markus Keller (Ihr IAM-Experte)