iTentity erklärt:

Was ist eigentlich IAM?

Thema:
Active Directory
Management

Teil IV

iTentity erklärt:

Was ist Active Directory Management?

Active Directory Management (ADM) im Identity & Access Management bezieht sich auf die Verwaltung und Organisation von Benutzerdaten, Gruppen, Computern und Ressourcen innerhalb eines Netzwerks.

ADM ermöglicht es Unternehmen, die Zugriffsrechte und Berechtigungen von Benutzern zentral zu steuern, um die Sicherheit und Effizienz in der IT-Infrastruktur zu gewährleisten.

Es ist ein zentraler Bestandteil im IAM, da es hilft, den Zugriff auf Systeme und Anwendungen zu regulieren und die Einhaltung von Sicherheitsrichtlinien sicherzustellen.

iTentity erklärt:

Warum ist Active Directory Management wichtig?

Zentralisierung von Benutzeridentitäten:
Active Directory (AD) fungiert als zentrale Datenbank für Benutzeridentitäten und Zugriffsrechte in einer Windows-Umgebung. Durch effektives AD-Management können Unternehmen die Verwaltung ihrer Benutzeridentitäten zentralisieren und vereinfachen.

Effiziente Bereitstellung & Verwaltung von Ressourcen:
Mit AD können Unternehmen Benutzerkonten, Gruppenrichtlinien, Sicherheitsgruppen und andere Ressourcen effizient bereitstellen und verwalten, was die Produktivität erhöht und die Betriebskosten senkt.

iTentity erklärt:

Warum ist Active Directory Management wichtig?

Sicherheitskontrolle und Zugriffsverwaltung:
AD ermöglicht es Unternehmen, Zugriffsrechte granular zu steuern und sicherzustellen, dass Benutzer nur auf die Ressourcen zugreifen können, die für ihre Aufgaben erforderlich sind. Dies trägt zur Stärkung der Sicherheit und zur Minimierung von Sicherheitsrisiken bei.

Integration in anderen Systemen und Anwendungen:
AD kann nahtlos mit anderen IAM- und Sicherheitssystemen integriert werden, um eine ganzheitliche Sicherheitslösung zu schaffen und die Effizienz der IT-Infrastruktur zu verbessern.

iTentity erklärt:

Wie funktioniert es im IAM?

Benutzerverwaltung:
Erstellen, ändern und löschen von Benutzerkonten im Active Directory, und deren Zugriffsrechte und Gruppenzugehörigkeiten verwalten.

Gruppenmanagement:
Erstellen und Verwalten von Sicherheitsgruppen und Verteilergruppen, um Zugriffsrechte auf Ressourcen zu organisieren und zu steuern.

Richtlinienverwaltung:
Definieren und implementieren von Gruppenrichtlinien, um Sicherheitsrichtlinien, Passwortrichtlinien und andere Einstellungen für Benutzer und Computer zu konfigurieren.

iTentity erklärt:

Wie funktioniert es im IAM?

Überwachung und Auditierung:
Überwachen & protokollieren von Benutzeraktivitäten und Zugriffsereignisse im Active Directory, um die Sicherheit zu erhöhen und Compliance-Anforderungen zu erfüllen.

I**ntegration in IAM-Lösungen:**
Integration von Active Directory nahtlos mit anderen IAM- und Sicherheitssystemen, um eine ganzheitliche Sicherheitslösung zu schaffen und die Effizienz der Zugriffsverwaltung zu verbessern.

In der nächsten und letzten Ausgabe der Reihe “Was ist eigentlich IAM?”, erfahrt ihr mehr über Identity Governance.