iTentity erklärt:

Was ist eigentlich IAM?

Thema:
Access Management

Teil II

iTentity erklärt:

Was ist Access Management im IAM?

Access Management im IAM bezieht sich auf die Verwaltung und Kontrolle der Zugriffsrechte von Benutzern auf verschiedene Anwendungen, Systeme und Daten innerhalb einer Organisation.

Es umfasst die Identifizierung, Authentifizierung, Autorisierung und Überwachung von Benutzerzugriffen, um sicherzustellen, dass nur autorisierte Benutzer auf die richtigen Ressourcen zugreifen können.

iTentity erklärt:

Warum ist Access Management wichtig?

Sicherheit:
Durch die strikte Kontrolle von Benutzerzugriffen können Sicherheitsrisiken minimiert und Daten vor unbefugtem Zugriff geschützt werden.

Compliance:
Access Management hilft bei der Einhaltung von Compliance-Vorschriften, indem es sicherstellt, dass der Zugriff auf sensible Daten und Systeme nur autorisierten Benutzern gewährt wird.

iTentity erklärt:

Warum ist Access Management wichtig?

Effizienz:
Durch die Automatisierung von Zugriffsprozessen können Unternehmen Zeit und Ressourcen sparen und gleichzeitig die Produktivität ihrer Mitarbeiter steigern.

Transparenz und Nachvollziehbarkeit:
Durch die Protokollierung und Überwachung von Benutzerzugriffen können Unternehmen ein umfassendes Bild davon erhalten, wer auf welche Ressourcen zugegriffen hat und zu welchem Zeitpunkt.

iTentity erklärt:

Wie funktioniert Access Management im IAM?

Identifizierung und Authentifizierung:
Benutzer werden identifiziert und authentifiziert, um sicherzustellen, dass sie diejenigen sind, für die sie sich ausgeben.

Autorisierung:
Basierend auf den identifizierten Benutzern und ihren Rollen werden Zugriffsrechte und Berechtigungen festgelegt.

iTentity erklärt:

Wie funktioniert Access Management im IAM?

Überwachung und Auditierung:
Benutzerzugriffe werden überwacht und protokolliert, um verdächtige Aktivitäten zu erkennen und zu untersuchen.

Zugriffsverwaltung:
Zugriffsrechte werden dynamisch verwaltet und aktualisiert, basierend auf den sich ändernden Anforderungen und Rollen der Benutzer.

In der nächsten Ausgabe erfahrt ihr mehr über Privileged Access Management.