iTentity erklärt:

Was ist eigentlich IAM?

Teil I

iTentity erklärt:

Was ist IAM?

IAM (Identity and Access Management) ist ein entscheidender Bestandteil der IT-Sicherheit, der Unternehmen dabei hilft, die digitalen Identitäten ihrer Benutzer (intern & extern) zu verwalten und den Zugriff auf Ressourcen zentral und effizient zu kontrollieren.

Durch eine zentrale Datenhaltung ermöglicht IAM es, Identitäten und Benutzerrechte transparent zu steuern und den Zugang zu sensiblen Daten und Systemen optimal abzusichern.

iTentity erklärt:

Warum ist IAM wichtig?

Zentralisierung und Transparenz:
Durch die zentrale Verwaltung von Identitäten und Benutzerrechten erhalten Unternehmen einen umfassenden Überblick über alle Zugriffsrechte. Dies ermöglicht es, Zugriffe schnell und präzise zu steuern, was die Sicherheit erheblich erhöht.

Schutz sensibler Daten:
IAM schützt wertvolle Daten vor unbefugtem Zugriff. Die zentrale Verwaltung reduziert das Risiko, dass Zugriffsrechte beispielsweise nach dem Ausscheiden eines Mitarbeiters weiterhin bestehen. Alle Zugriffe können zentral entfernt werden, was Sicherheitslücken schließt und Compliance-Anforderungen erfüllt.

iTentity erklärt:

Warum ist IAM wichtig?

Effizienz und Produktivität:
Automatisierte Zugriffsprozesse sparen Zeit und Ressourcen.

Sicheres Arbeiten aus der Ferne:
IAM gewährleistet, dass Mitarbeiter und Partner sicher auf Unternehmensressourcen zugreifen können – unabhängig vom Standort.

iTentity erklärt:

Was sind die Kernpunkte des IAM?

- Access Management
- Privileged Access Management
- Active Directory Management
- Identity Governance and Administration

Die Aufgaben der einzelnen Kernpunkte erklären wir euch in den nächsten Teilen unserer Wissensreihe.