iTentity erklärt:

Was ist eigentlich IAM?

Thema:
Privileged Access Management

Teil III

iTentity erklärt:

Was ist Privileged Access Management im IAM?

Privileged Access Management (PAM) im Identity and Access Management (IAM) ist ein entscheidender Schritt, um sensible Konten und privilegierte Zugriffe innerhalb einer Organisation effektiv zu schützen.

PAM umfasst beispielsweise Maßnahmen, wie die sichere Speicherung von Passwörtern, die Überwachung von Aktivitäten und die zeitlich begrenzte Vergabe von Zugriffsrechten, um sicherzustellen, dass privilegierte Konten nur für legitime Zwecke und in einem kontrollierten Rahmen verwendet werden.

iTentity erklärt:

Warum ist PAM wichtig?

Sicherheitsschicht für sensible Konten:
Privilegierte Konten wie Administrator- und Root-Konten haben weitreichende Zugriffsrechte und stellen ein hohes Sicherheitsrisiko dar. Privileged Access Management (PAM) kontrolliert und überwacht den Zugriff auf diese Konten. Ein zentrales Merkmal von PAM ist die Möglichkeit, administrative Zugriffe zu ermöglichen, ohne das Passwort preiszugeben. Die Passwörter sind sicher hinterlegt und werden automatisch eingetragen, sodass sich Benutzer als Administrator anmelden können, ohne das Passwort zu kennen. Dies schützt sensible Zugangsdaten und erhöht die Sicherheit erheblich.

iTentity erklärt:

Warum ist PAM wichtig?

Schutz vor Insider-Bedrohungen:
PAM reduziert das Risiko von Insider-Bedrohungen, indem es den Zugriff auf sensible Ressourcen auf autorisierte Benutzer beschränkt und unbefugte Zugriffe verhindert.

Compliance-Anforderungen erfüllen:
Viele Compliance-Vorschriften, wie PCI DSS und HIPAA, erfordern die Implementierung von robusten Privileged Access Management-Lösungen, um die Sicherheit von sensiblen Daten zu gewährleisten.

iTentity erklärt:

Warum ist PAM wichtig?

Reduzierung von Angriffsflächen:
Durch die Begrenzung und Überwachung des Zugriffs auf privilegierte Konten minimiert PAM potenzielle Angriffsflächen und verringert das Risiko von Datenschutzverletzungen und Datenmissbrauch.

iTentity erklärt:

Wie funktioniert PAM im IAM?

Identifikation privilegierter Konten:
Identifizieren von allen privilegierten Konten innerhalb einer Organisation, einschließlich Administrator-, Root- und Servicekonten.

Zugriffsbeschränkung:
Begrenzen von Zugriff auf privilegierte Konten auf autorisierte Benutzer und Anwendungen und Umsetzen des Prinzips des geringsten Privilegs.

iTentity erklärt:

Wie funktioniert PAM im IAM?

Multi-Faktor-Authentifizierung (MFA):
Implementieren von zusätzlichen Sicherheitsmaßnahmen, wie MFA, um den Zugriff auf privilegierte Konten weiter abzusichern.

Überwachung und Protokollierung:
Überwachen und protokollieren von allen Zugriffs-aktivitäten auf privilegierte Konten, um verdächtige Aktivitäten frühzeitig zu erkennen und zu untersuchen.

iTentity erklärt:

Wie funktioniert PAM im IAM?

Regelmäßige Überprüfungen und Audits:
Durchführen regelmäßiger Überprüfungen und Audits der Privileged Access Management-Richtlinien und -Prozesse, um sicherzustellen, dass sie den aktuellen Sicherheits-anforderungen entsprechen.

In der nächsten Ausgabe erfahrt ihr mehr über Active Directory Management.