Identity & Access Management ohne Enterprise-Budget

– Minimal-IAM-Referenzarchitektur –

Eine Minimal-IAM-Referenzarchitektur beschreibt die grundlegenden Komponenten, die Organisationen benötigen, um digitale Identitäten kontrolliert zu verwalten. Ziel ist kein komplexes Enterprise-IAM, sondern eine pragmatische Struktur, die mit vorhandenen Plattformen und überschaubarem Aufwand umgesetzt werden kann.

1. Zentrale Identitätsquelle

Im Zentrum der Architektur steht ein zentrales Identitätsverzeichnis, das als Single Source of Identity fungiert. Dieses System verwaltet Benutzerkonten, Gruppen, Rollen und grundlegende Identitätsattribute. Alle Benutzeridentitäten werden in diesem System angelegt und verwaltet. Typische Beispiele:

- Active Directory
- Microsoft Entra ID
- Google Workspace Identity

2. Identity Provider (IdP)

Der Identity Provider übernimmt die Authentifizierung von Benutzern und stellt Identitätsinformationen für Anwendungen bereit. Der Identity Provider dient als zentraler Zugangspunkt für Anwendungen. Die Aufgaben des Identity Providers:

- Benutzeranmeldung
- Multi-Factor Authentication
- Single Sign-On
- Ausgabe von Authentifizierungstokens

Typische Protokolle:

- SAML
- OpenID Connect
- OAuth 2.0

3. Anwendungen und Systeme

Unternehmensanwendungen und Cloud-Dienste werden an den Identity Provider angebunden. Dadurch können Benutzer sich über Single Sign-On anmelden. Die Authentifizierung erfolgt über den zentralen Identity Provider. Typische Systemkategorien sind:

- SaaS-Anwendungen (CRM, Kollaboration, HR-Systeme)
- interne Webanwendungen
- Infrastruktur-Systeme (Server, Netzwerkdienste)

4. Rollen- und Gruppenstruktur

Berechtigungen werden über Rollen oder Gruppen gesteuert, nicht über individuelle Benutzerzuweisungen. Jede Rolle definiert, auf welche Systeme oder Anwendungen Benutzer Zugriff erhalten. Beispiele für Rollen:

- Vertrieb
- Buchhaltung
- IT-Administration
- Management

5. Privileged Access Management

Privilegierte Konten werden besonders geschützt. Administratorzugriffe sollten nur bei Bedarf aktiviert werden. Zentrale Maßnahmen sind:

- Trennung von Standard- und Admin-Konten
- Passwortsafe oder Secrets Management
- Just-in-Time-Administratorrechte
- Protokollierung administrativer Aktivitäten

6. Logging und Monitoring

Alle sicherheitsrelevanten Ereignisse werden protokolliert. Protokolle sollten zentral gesammelt und regelmäßig überprüft werden. Dazu gehören:

- Anmeldeereignisse
- MFA-Nutzung
- Änderungen von Benutzerkonten
- Administrative Aktionen

7. Lifecycle-Prozesse

Die Verwaltung von Identitäten folgt strukturierten Prozessen, wobei diese Prozesse idealerweise durch HR-Systeme oder Workflow-Systeme unterstützt werden:

- Joiner – neue Benutzerkonten werden angelegt
- Mover – Rollen und Berechtigungen werden angepasst
- Leaver – Benutzerkonten werden deaktiviert

Auch mit begrenzten Ressourcen lässt sich so eine stabile Grundlage für sicheres Identity & Access Management schaffen. Diese Architektur ermöglicht es Organisationen:

- Identitäten zentral zu verwalten
- Zugriffe kontrolliert zu vergeben
- privilegierte Konten zu schützen
- Authentifizierung zu standardisieren
- IAM-Prozesse auditfähig zu gestalten

Mehr zum Thema IAM:

Der vollständige Leitfaden „Identity & Access Management ohne Enterprise-Budget“.

🛒 Jetzt bei Amazon bestellen