AIRLOCK IAM

Zugriff für alle Benutzer. Reibungslos.

Im Airlock Secure Access Hub wird Airlock IAM meist in Kombination mit Airlock WAF und Airlock API Gateway eingesetzt. Die Aufgabe von Airlock IAM ist es, Benutzer zu verwalten, zu authentifizieren und die entsprechenden Identitätsinformationen in der passenden Form an die gewünschte Applikation zu übermitteln.

Consumer IAM (cIAM)

Airlock IAM verwaltet als cIAM System Benutzer, die von aussen auf Applikationen und Services zugreifen wollen und ist entsprechend für grosse Benutzerzahlen skalierbar. Zudem bieten die cIAM Lösung eine nahtlose User Experience durch optimierte und integrierte Benutzerschnittstellen für Onboarding und Self-Services. Der Umgang mit Social Idenitites (BYOI) und eine hohe Flexibilität beim Authentisierungsvorgang sind einer der entscheidenden Pluspunkte von Airlock IAM.

Starke Authentisierung mit starker Auswahl

Damit ein Login nicht an den Schwächen eines einzigen Authentisierungsmittels leidet, wird meist eine starke Authentisierung mit zwei Faktoren (auch MFA genannt) eingesetzt. Flexible Kombinationsmöglichkeiten sind dabei besonders wichtig.

Airlock IAM ist mit verschiedenen Lösungen kompatibel und kann beispielsweise mittels Passwort, Mobile TAN (mTAN), Matrix-Karte, E-Mail-OTP, Kobil SecOVID, OneSpan Digipass (Vasco), Swisscom Mobile ID (Mobile Signature Services), Client-Zertifikaten wie X.509 oder SuisseID sowie Cronto- Sign von OneSpan und vielen anderen Methoden eingesetzt werden.

Adaptive Authentifizierung

Airlock IAM kann den Benutzerzugriff auch auf unterschiedliche Weise dynamisch steuern und bietet für alle Bedürfnisse die optimale Abstimmung zwischen Sicherheit und Benutzerfreundlichkeit. Insbesondere kann die aktuelle Situation des Zugriffs (z.B. vom Arbeitsplatz, von zuhause oder unterwegs) und die Historie eines Benutzers dabei berücksichtigt werden. Es werden u.a. folgende Konzepte unterstützt:

- RBAC/ABAC (role-/attribute-based access control)
- Risikobasierte Authentifizierung
- Re-Authentifizierung und Timeout-Funktionen auf einzelnen Rollen
- Umsetzung komplexer Access Policies mittels Regeln und logischen Operatoren

Single Sign-On (SSO) Standards

Der Secure Access Hub entkoppelt die einzelnen Zugriffe von den Applikationen und kann darum als smarte Identitätsweiche fungieren. Je nachdem wo ein Zugriff hingeleitet wird, kann die Identität des authentisierten Benutzers anders repräsentiert werden. Dadurch wird ein transparenter Single Sign-on möglich, der hohe Sicherheit mit hoher Benutzerakzeptanz verbindet.

Airlock IAM unterstützt diverse SSO Standards und Formate wie SAML Assertions, Kerberos Tickets, OAuth 2.0 Tokens, OpenID Connect Tickets, HTTP Headers, URL Tickets, etc..

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zürich |Telefon: +41 44 268 89 00 | E-Mail: info@airlock.com

Social Registration und BYOI

Benutzer wollen sich aber auch schnell und unkompliziert registrieren und einloggen. Dabei möchten sie bestehende Identitäten wiederverwenden, um nicht noch mehr Passwörter einrichten zu müssen. Wenn Benutzer ihre Identitäten für den Zugriff von aussen mitbringen, spricht man von BYOI (Bring Your Own Identity). Die Alternative zum Passwortwirrwarr sind die Standards OAuth und OpenID Connect.

Diese erlauben die Wiederverwendung von Benutzeridentitäten und geben dem Benutzer die Kontrolle über deren Verwendung. Falls man sich dennoch nicht gänzlich auf einen externen Identity Provider wie z.B. Facebook verlassen möchte, kann Airlock IAM diese Identitäten mit einem zweiten Faktor ergänzen damit eine starke Authentifizierung möglich wird.

Umfassende User Self-services

Die Einrichtung von Benutzerkonten und Anmeldeprozesse führen bei Anwendern zu viele Fragen. Eine zielgerichtete Benutzerführung mit optimierter User Experience ist daher von höchster Bedeutung, um zu verhindern, dass der Helpdesk mit Anfragen überschwemmt wird. Airlock IAM bietet eine Vielzahl von optimierten und integrierten UIs für Anmeldung, Onboarding und Self-services.

Dazu gehören Kiosk- und Portalfunktionen für die Verwaltung eigener Daten, selbständige Registrierung (auch über Social-Media-Kanäle) sowie die Verwaltung entsprechender Konten und Tokens inklusive Migrations-Workflows. Mit dem integrierten Consent Management können zudem DSGVO-Anforderungen für angebundene Anwendungen schnell und unkompliziert gelöst werden.

Deployment

Docker Image, Self-Contained Application

Funktionen:

- **Benutzerauthentifizierung**
  - Passwort Authentifizierung
  - Grosse Auswahl an zweiten Faktoren für starke Authentifizierung
  - X.509 Client Zertifikate
  - Adaptiv und risiko-basiert
  - «Remember Me»
  - RADIUS Server
  - Workflow-basiert
- **Request Authentifizierung**
  - Authentifizierung von REST Calls
  - JWT, Basic Auth, Client Zertifikate
- **Benutzerverzeichnisse:** Datenbanken, LDAP, MSAD
- **Benutzer-, Token- und Rollenverwaltung inkl. Helpdesk-Tool**
- **Benutzer Self-Services**
  - Password-Reset
  - Registrierung von zweiten Faktoren
  - Verwaltung von zweiten Faktoren
  - Kiosk- und Portalfunktion für eigene Benutzerdaten
- **Single Sign-on (SSO)**
  - Grosse Anzahl unterstützter Protokolle
- **Login REST API**
- **Admin REST API**
- **SAML 2.0 IdP und SP**
- **OAuth 2 und OpenID Connect**
  - Als Authorization Server / OP
  - Als Client / RP
  - Authorization Code Flow, Implicit Flow, Client Credentials Flow
  - Dynamic Client Registration, Discovery
  - Diverse weitere Funktionen
- **Social Registration und Social Account Linking**
- **GDPR Consent Enforcement**
- **Mandantenfähig**
- **Hoch skalierbar**
- **Sicherheit auf Bankenniveau**
- **Individuell erweiterbar**

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zürich |Telefon: +41 44 268 89 00 | E-Mail: info@airlock.com