

Success Story

Gruppenweite IAM Strategie & Identity-Fabric-Architektur

Ausgangslage

Baloise stand vor der Herausforderung, ihre historisch gewachsene, produktorientierte IAM-Landschaft in eine ganzheitliche, gruppenweite End-to-End-Disziplin zu überführen.

Ziel war der Aufbau einer zentralen IAM-Kompetenz, die Security, Compliance und Business Enablement gleichermaßen adressiert – und IAM als skalierbaren Enterprise Service etabliert.

Dafür sollten:

- eine Zero-Trust-basierte IAM-Strategie definiert,
- eine konsistente Zielarchitektur entwickelt,
- und eine gruppenweite Governance organisatorisch verankert werden.

Im Fokus standen eine stärkere Risikosteuerung, höhere Transparenz sowie die Fähigkeit, hybride Applikationen effizient und standardisiert anzubinden.



Kunde

Baloise Versicherung AG



Scope

Group IAM / Hybride Applikationslandschaft



Bausteine

IAM Strategie, Governance & Organisation, Zielarchitektur, risikobasiertes IAM, Integration Factory

Strategische Entscheidung

Statt punktueller Tool-Optimierungen entschied sich Baloise bewusst für ein strategisches Zielbild:



Ein Zero-Trust-orientiertes IAM-Operating-Modell mit klaren Policies, definierten Verantwortlichkeiten und einer skalierbaren Identity-Fabric-Architektur.



IAM sollte nicht länger als Technologieprojekt verstanden werden – sondern als steuerbarer, wertorientierter Enterprise Service.

Vorgehen

Das Programm wurde in Streams aufgebaut, um Governance, Architektur und Umsetzung parallel zu operationalisieren und gleichzeitig mittels dedizierten Aufbaus einer Community of Practice und Workshops die Akzeptanz in den Landesgesellschaften zu sichern.

Zentrale Bausteine

1. Standortbestimmung

- Maturity- und Gap-Analyse über Governance
- Organisation, Prozesse & Technologien

3. Identity-Fabric-Zielarchitektur

Aufbau einer serviceorientierten Architektur mit:

- klar definierten Integrationsstandards und Just-in-Time Mechanismen
- standardisierten Inbound und Outbound Integrationspattern

2. Strategie & Roadmap

- Definition der Zero-Trust-IAM-Strategie mit Target Capabilities
- Priorisierung der Roadmap und passende Programmstruktur

4. Integration Factory & Knowledge Hub

Etablierung eines skalierbaren Factory-Ansatzes mit:

- Integrations-Entscheidungsbaum inkl. Blueprints & Templates
- Self-Service Enablement inkl. Quality Gates

Gruppenweite IAM Strategie & Identity-Fabric-Architektur

Ergebnisse & Impact

Die Initiative schafft ein gruppenweit konsistentes IAM-Zielbild und etabliert operative Fähigkeiten, um IAM nachhaltig, skalierbar und risikobasiert zu steuern.

Konkreter Mehrwert

- Einheitliche Architektur- und Prozessstandards über Länder-/Business-Grenzen hinweg
- Schnelleres, gleichförmiges Applikations-Onboarding auf Basis Security-by-Design statt Sonderlösungen
- Audit-Readiness durch nachvollziehbare Policies, KPIs und Operating Model
- Risikosteuerung durch IAM-Scoring sowie erhöhte Transparenz durch Application Dashboard (Analytics/Reconciliation, priorisierte Remediation) für zielgerichtete und messbare IAM-Investitionen

IAM wird damit von einer technischen Disziplin zu einem steuerbaren, wertorientierten Enterprise Service weiterentwickelt.

Lessons Learned

Drei zentrale Erkenntnisse – relevant für jedes regulierte Unternehmen mit hybrider IAM-Landschaft:

1.

Frameworks schaffen Orientierung – Mehrwert entsteht erst durch Operationalisierung.

Strategiemodelle müssen in betreibbare Services, Standards und Prozesse übersetzt werden.

2.

Identity Fabric statt Tool-Inseln.

Ein Value-Stream-orientierter Ansatz verhindert Parallelstrukturen und skaliert Integrationen deutlich effizienter.

3.

Governance braucht Enablement.

Akzeptanz entsteht nicht durch Vorgaben, sondern durch Templates, Factory-Services und partner-schaftliche Beratung – so dass sie in der Organisation auch ankommen.

Testimonial

«Blackdot hat uns geholfen früh die richtigen Leitplanken zu setzen: Den Aufbau einer effizienten Governance, die Etablierung eines effektiven Risiko Managements und die Definition einer holistischen Zielarchitektur vor einzelnen Tooling-Inseln. Das hat es uns ermöglicht, IAM als Service zu etablieren und erste Schritte für Zero Trust in der Praxis umzusetzen.»

Basel

Blackdot AG
Rittergasse 35, 4051 Basel, Schweiz
office@blackdot.swiss, +41 61 312 07 07

Wien

Blackdot GmbH
Servitengasse 5/16, 1090 Wien, Österreich
office@blackdot.at, +43 1 99 77 258

Hamburg

Blackdot GmbH
Neuer Wall 10, 20354 Hamburg, Deutschland
office@blackdot.de, +49 40 822 1532 53