IAM - Introduction

Eine Einführung ins IT Security Thema
Identity & Access Management

Autor: **Mike Dätwyler**

E-Mail: contact@mike-daetwyer.ch

Website: mike-daetwyler.ch

Stand: April 2023

Inhaltsverzeichnis

Basics

Definition: IAM

Der Begriff IAM, ausgeschrieben **Identity & Access Management**, steht für die zentrale Verwaltung von Identitäten und Zugriffsberechtigungen. Es dient als eine zentrale Zugriffskontrolle, welche jegliche Identitäten und Accounts in einer Organisation, einem Netzwerk, verwaltet.

Mithilfe eines IAM-Systems kann so die Arbeit von bspw. AD-Mitarbeitern entlastet werden. Dies ergibt sich durch die aus dem IAM entstehende Automatisierung.

Die Evaluierung eines solchen IAM-Systems ist, typisch für Sicherheit, mit hohem Aufwand und Kosten verbunden. Deshalb wird es in der Praxis eher in grösseren Unternehmen aufzufinden sein. Ein weiterer Grund dafür ist, dass in Grossunternehmen viel mehr Mitarbeiterwechsel passieren – seien es Neuzugänge, Kündigungen oder interne Stellenwechsel.

Eine Person (Mitarbeiter) wird als Identität, Identity, angesehen. Jegliche Berechtigungen und Zugänge einer Person sind mit dieser Identity verknüpft und somit auch alle Accounts.

Definition: IAG

Mit IAG, ausgeschrieben **Identity & Access Governance**, kann man IAM noch besser ausführen. Man kann sich einen genaueren Einblick verschaffen, wer sich wo fälschlicherweise versucht hat einzuloggen/etwas auszuführen. IAG verlinkt Identities mit Applikationen und Daten, um feststellen zu können, wer Zugriff zu was hat.

Wenn jemand Unautorisiertes versucht ins System zukommen, kann IAG feststellen, ob eine Gefahr droht und den Systemadministrator alarmieren.

Zusätzlich hilft IAG bei der Automatisierung des Entfernens von Zugriffsberechtigungen. Dies tut es, indem es analysiert, ob der User zuvor dazu berechtigt war oder nicht.

Wozu IAM?

Mit IAM schafft man Automatisierung in einer Organisation, einem Netzwerk. Somit schafft man eine effizientere Umgebung, in welcher z.B. kein AD-Mitarbeiter mehr von Hand neue User eintragen muss. Zusätzlich erhält man einen genaueren Überblick über die Zugriffsberechtigungen die IT-Security in der Organisation wird erhöht.

Wie vorhin bereits erwähnt, wenn ein neuer Mitarbeiter seinen ersten Tag hat, wird er noch nicht direkt produktiv arbeiten können. Dies liegt in erster Hand nicht einmal unbedingt nur am fehlenden Knowhow, sondern an den Zugriffsberechtigungen. Sei es dabei nur schon das Windows Login, aber dann auch in der benötigten Software oder dem Online-Portal.

Wichtig ist hierbei, dass das Eintritts- wie auch das Austrittsdatum bekannt und hinterlegt ist, sowie aber auch, dass lediglich die benötigten Zugriffsberechtigungen erteilt werden.

Durch IAM wird dieser Prozess beschleunigt und der Mitarbeiter wird nicht mehrere Tage umsonst bezahlt.

Vorteile

- Automatisierung
    - Administratoren müssen nicht mühsame, eintönige Arbeit vollrichten
        - bspw. jeden einzelnen Mitarbeiter inkl. Berechtigungen eintragen
    - schnellere Prozesse
- bessere Kontrolle/Übersicht über Zugriffsberechtigungen
    - erhöhte Nachvollziehbarkeit
- höhere Security

Nachteile

- hohe Kosten
- Evaluierung mit Aufwand verbunden
- Spezialisten benötigt
- Risiko aufgrund von Automatisierung
    - wenn bspw. in Rolle falsche Berechtigungen gesetzt sind und dann 5'000 Mitarbeiter diese falsche Rolle erhalten

IAM Stakeholder

Interessensgruppen

Interesse an einer Einführung eines IAM-Systems haben verschiedene Gruppen.

Einerseits wären das hierbei externe Einflüsse. Sprich, bspw. bei einer Bank könnten Regulationen von extern ein Grund für die Einführung eines IAM-Systems sein. Weiter gibt es aber sicherlich auch auf interner Seite Interesse an solche einer Implementation.

Um die Automatisierung des Unternehmens zu fördern, möchte vielleicht die Geschäftsleitung, dass ein IAM-System eingeführt wird. Die Informatik selbst könnte aber auch ein gewisses Interesse zeigen, sei es ein Vorschlag von einem Mitarbeiter oder gar des Informatik-Leiters. Spezifischer wären das vielleicht dann bspw. der Service Desk oder das Security Office bzw. der CISO.

Weiter haben sicher auch Mitarbeiter des Finance Accountings, vom HR aber auch die Ziel-System-Verantwortlichen ein gewisses Interesse an der Nutzung von IAM.

Auftraggeber

Auftraggeber werden hierbei meist aus interner Quelle stammen, da externe Einflüsse meist nur als eine Empfehlung abgegeben werden.

Hinter IAM muss ein gewisses Konzept stecken, denn ohne ein solches würde die Implementierung keinen Sinn ergeben. Darin werden dann je nach Grösse des Unternehmens Informatik oder auch die Geschäftsleitung involviert sein.

Anforderungen stellen hierbei vor allem die Interessensgruppen wie z.B. das HR oder der Service Desk.

Umsetzung

Die Umsetzung kann hierbei durch Externe ausgeführt werden. In einem Unternehmen, welches eine etwas grössere interne Informatik hat, wird es oft durch ein internes Informatik-Team ausgeführt.

Das Gleiche gilt dann auch für den weiteren Betrieb des IAM-Systems.

Governance

Die IT wird mit der Unternehmensstrategie verknüpft. Dies passiert durch Governance, welche einen regulatorischen Rahmen bildet. Mit Governance wird also sichergestellt, dass die IT strategisch mit einem Plan eingesetzt wird und dadurch die Unternehmensziele optimal unterstützen kann.

Hierbei geht es also um die **Festlegung** von Rahmenbedingungen und Regulatoren.

Compliance

Compliance in der IT beschreibt in der Unternehmensführung die Einhaltung der gesetzlichen oder auch vertraglichen Regelungen im Bereich der IT. Der Begriff stammt aus der BWL und ist die Umschreibung für die Regeltreue von Unternehmen, was so viel wie die Einhaltung von Gesetzen und Richtlinien bedeutet.

Hierbei geht es also um die **Einhaltung** von Rahmenbedingungen und Regulatoren.

Rahmenbedingungen

Generelle Rahmenbedingungen

Das IAM muss das **Need-To-Know-Prinzip** einhalten. Sprich, jede Identität soll nur so viele Berechtigungen erhalten, wie sie auch benötigt.

Berechtigungen sollen auf Rollen basieren und regelmässig überprüft werden.
Diese Berechtigungen dürfen sich nicht im Widerspruch befinden, das heisst Person X darf nicht Owner einer Gruppe Y sein und sich diese selbst zuteilen und bestätigen. Dies nennt man Segregation of Duties (SoD).

Regelmässige Überprüfungen, Nachvollzieh- und Auswertbarkeit sind wichtige Rahmenbedingungen fürs IAM. Je kritischer die Berechtigungen sind (Admin-Rechte = sehr kritisch), desto mehr Audits (Überprüfungen/Auswertungen) müssen gemacht werden.
Zudem muss in einem IAM-System die Passwortkomplexitätsanforderung gewährleistet sein. (Bspw. Gross/Klein, Sonderzeichen, Ziffer, 8 Stellen)

Gesetzliche Rahmenbedingungen (DSGVO)

Schweizer Unternehmen müssen sich an das **Schweizer Datenschutzgesetz** halten. Das Unternehmen soll auf der Website umfassend und transparent darüber informieren, welche Personendaten zu welchen Zwecken bearbeitet werden. Die Stichworte hier sind hierbei: Transparenz, Verhältnismässigkeit, Zweckbindung und die Rechte der Betroffenen.

In der Dokumentationspflicht **Verzeichnis von Verarbeitungstätigkeiten (VTT)** sind alle Datenverarbeitungen, die persönliche Daten betreffen, aufzulisten. Es dient der Dokumentation und Transparenz. Wenn jegliche Verarbeitungen im eigenen Unternehmen, welche passieren, bekannt sind, kann auf Anfragen von Betroffenen schnell und präzise geantwortet werden. Das Verarbeitungsverzeichnis muss auf Anfrage auch der Aufsichtsbehörde vorgelegt werden können. Dabei wird vorausgesetzt, dass es schon lange existiert und kontinuierlich gepflegt wird. Eine lange Frist kann man von der Behörde für die Vorlage davon nicht erwarten.
Dies gilt für alle Verantwortlichen von Datenverarbeitungen.

Die **Informationspflicht** bedeutet, dass man Personen ihre Daten vorlegen können muss. Sprich, wer was wann und bei welcher Gelegenheit über die betroffene Person weiss.

Wichtig ist noch anzumerken, dass Personendaten **Eigentum** der jeweiligen Person bleiben. Aus diesem Grund gibt es das **Auskunftsrecht**, welches beinhaltet, dass eine Person das Recht besitzt, ohne jegliche formale Anträge oder Begründungen eines verantwortlichen Auskunft über die eigenen Daten verlangen zu dürfen.

Die **Datenschutz-Grundverordnung** (Datensicherheit) orientiert sich an der Schutzbedürftigkeit der einzelnen gespeicherten personenbezogenen Daten. Es muss also eine Schutzbedarfsfeststellung vorgenommen werden, indem der jeweilige Schutzbedarf der unterschiedlichen personenbezogenen Daten ermittelt wird. Dabei werden zunächst typische Schadenszenarien ermittelt und anschliessend der Schutzbedarf für die einzelnen personenbezogenen Daten abgeleitet.

Ein weiterer Regulator kann z.B. das Unternehmen, in dem IAM eingesetzt wird, oder ein externer Partner sein.

Analogien: Governance Korrelationen

Governance legt die **Rahmenbedingung** «DSGVO» fest, in welcher die Informationspflicht geschrieben steht. Das heisst es wird festgelegt, dass man Personen immer ihre Daten vorlegen können muss. **Compliance** muss sich nun darum kümmern, dass man Personen ihre Daten immer vorlegen kann. Mit Hilfe von **Audits** (=Überprüfungen) wird kontrolliert, ob die gesetzten (Governance) Rahmenbedingungen eingehalten (Compliance) werden.

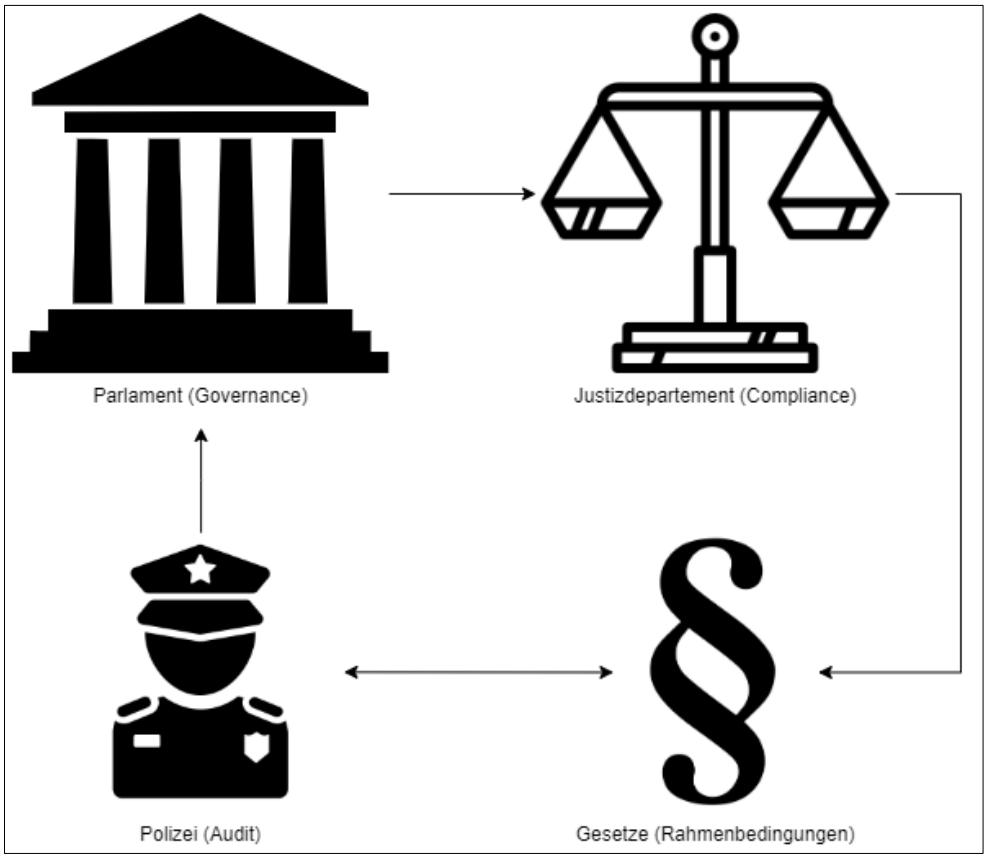

Abbildung 2: Analogie: Governance Korrelation (Dätwyler, 2023)

IAM Schnittstellen

IAM als Drehscheibe

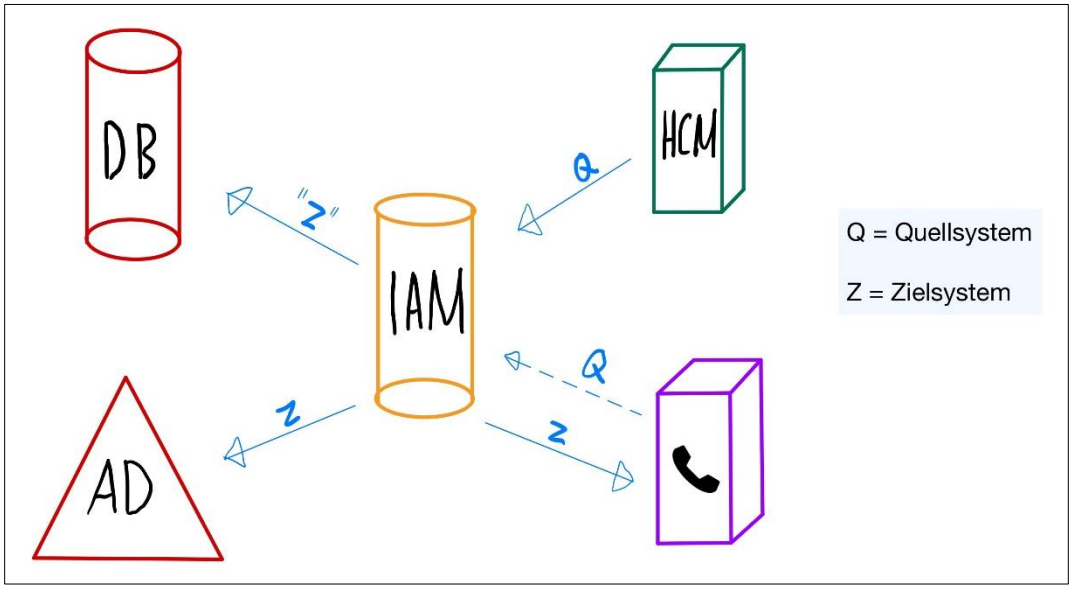

Abbildung 3: IAM als Drehscheibe (Dätwyler, 2023)

Aufbau eines IAM-Systems

Ein IAM-System ist quasi eine Datenbank. Diese ist mittels sogenannter Konnektoren mit diversen Zielsystemen verknüpft. Zielsysteme, bzw. Schnittstellen sind hierbei bspw. das Active Directory, LDAP, Exchange, SharePoint, ein HCM-System, aber auch Cloud-Lösungen wie Azure, G-Suite oder O365. Mittels SCIM ist es ebenfalls möglich eine Verbindung zu Cloud Plattformen wie die von SAP oder Jira herzustellen.

Das IAM-System bezieht z.B. Personendaten vom HCM-System und gibt diese dann weiter zum Active Directory. (Siehe Skizze)

Ein IAM-System kann aus einer Main-DB und einer History-DB bestehen. In der Main-DB werden jegliche Objekte gespeichert, während in der History-DB lediglich alle Änderungen und gelöschte Elemente festgehalten werden. Daran verknüpft sind dann unter anderem ein Webserver, über welchen dann der Access Request (User-Interface) gehostet wird, wie aber auch mehrere Job-Server. Diese Job-Server bearbeiten die Aufträge, welche über das IAM-System ausgelöst werden. Diese Aufträge wiederum können Einfluss auf bspw. das AD oder Exchange haben.

Datenquellen und deren Anbindung

Von woher kommen die Daten ins IAM?

Die Daten können einerseits aus einem Telefonsystem, einem Exchange Server oder natürlich auch von einem HCM-System stammen.

Bsp.: Die Daten werden als CSV von einem HCM-System exportiert. Mit dem einem Synchronisationstool wird das CSV dann anschliessend ins IAM-System importiert, indem man eine **Synchronisation** ausführt.

Zielsysteme

Beispiel-Systeme wären:

- Active Directory / LDAP
- Datenbanken
- Exchange-Server
- Telefonie-Server
- Cloud Plattformen
- SAP

Wichtige Daten fürs IAM

Wichtige Daten für ein IAM-System sind:

- Vor- und Nachname
- Personalnummer
- Eintrittsdatum
- Austrittsdatum

Was ist ein Konnektor?

Ein Konnektor ist eine Verbindung zu einem System oder einer Anwendung, welche die Synchronisation von Informationen ermöglicht. Somit können schnell und korrekt Änderungen im Bereich des IAMs vorgenommen werden. Dabei werden diese über mehrere Systeme hinweg synchronisiert, ohne dass ein IAM-Admin jegliche Accounts manuell updaten muss.

Ein **Quell-Konnektor** kreiert die Verbindung zu einem Zielsystem, in welchem die Mitarbeiterinformationen gespeichert sind. Die Daten werden von dort abgerufen und in andere Systeme übertragen. Ein Beispiel-System wäre hierbei das HCM-System.

Ein **Ziel-Konnektor** stellt eine Brücke zwischen dem IAM-System und dem Zielsystem, an welches die Informationen/Änderungen (Accounts) übertragen werden sollen, dar. Wenn nun also bspw. ein HCM-System als Quellsystem verwendet wird, können dort die Personendaten eines Mitarbeiters hinzugefügt werden und mittels des Quell-Konnektors ans IAM-System geleitet werden. Die mit dieser Person verknüpften Accounts können dann an alle Zielsysteme mittels Ziel-Konnektor übertragen werden. Wichtig dabei zu erwähnen ist, dass dieser Vorgang komplett automatisch durchläuft. Ein Beispiel-System wäre hierbei das AD oder Exchange.

Arten von Konnektoren

- CSV-Konnektor
- AD-Konnektor
- Azure AD-Konnektor
- DB-Konnektor
- LDAP-Konnektor
- Exchange-Konnektor
- SAP-Konnektor
- PowerShell-Konnektor

Bestandteile eines Konnektors

Ein Konnektor besteht aus:

- einem Connection String/Connection Parameter, welcher dafür da ist, das Zielsystem mit dem IAM zu verbinden. (Standort/Login Informationen mitgeben)
- einem Mapping, welches die einzelnen Objekte vom Zielsystem mit dem IAM matcht. (Bspw.: AD=Firstname | IAM=Prename)
- einem Workflow, welcher festhält, ob bspw. Daten, welche im IAM vorhanden sind, im Zielsystem jedoch nicht, ins Zielsystem provisioniert werden sollen, oder nicht. (Insert → Insert/Update/Delete für Synchronisierung und Provisionierung)
- einem Schedule, welcher beschreibt, wann welche Synchronisationen ausgeführt werden sollen.

De-/Provisierung

Im Gegensatz zur Synchronisierung, bei welcher Daten vom Zielsystem ins IAM übernommen werden, werden bei der Provisionierung Daten vom IAM ins Zielsystem geschrieben. Deprovisionierung beschreibt dann das Entfernen von Daten im Zielsystem. (wenn im IAM bspw. eine Löschung eines Accounts ausgeführt wird)

Automatismus im IAM

Rollen

Definition

In den einzelnen Zielsystemen wie z.B. das AD oder SAP, gibt es Berechtigungen. Diese kommen in Form von Gruppen und Roles. Ein AD-Account bspw. kommt mit hunderten von Berechtigungen daher, damit dieser überhaupt einigermassen einsetzbar ist. Ein Mitarbeiter benötigt dann aber nicht nur die Berechtigungen des ADs, sondern auch von anderen Systemen. Diese Menge an Berechtigungen, vor allem multipliziert mit der Anzahl von Zielsystemen, ergibt eine gewisse Unübersichtlichkeit.

Es gibt meistens mehrere Mitarbeiter in einem Unternehmen, welche dieselben Berechtigungen benötigten, was ein weiterer Grund ist, weshalb die manuelle Zuteilung etlicher Berechtigungen nicht sehr schmackhaft ist.

Aus diesem Grund gibt es Rollen. Rollen sind grundsätzlich ein Bundle von Berechtigungen. Sprich, wenn nun mehrere Mitarbeiter die gleichen Berechtigungen benötigen (zehn Service Desk Mitarbeiter) können sie sich einfach ein Bundle zuweisen lassen. (bspw. eine Geschäftsrolle "Service Desk")

Vorteile

Durch das Bündeln von Berechtigungen wird eine gewisse Einfachheit bereitgestellt, was schlussendlich zu Automatisierung führt. Zudem werden technische Begriffe gemieden, weshalb sie ebenfalls dadurch noch einfach zu managen sind. Es gibt dann also GRs wie Arzt, Jurist etc.

Ein weiterer Vorteil zeigt sich bei der Governance. Es ist viel einfacher eine Attestierung mit wenigen Rollen durchzuführen als mit tausenden von Berechtigungen.

Bsp.: Manager von Mitarbeiter X erhält eine Attestierungsaufforderung. Dieser soll angeben, ob Mitarbeiter X noch die GR "Arzt" benötigt oder nicht. Da der Manager weiss, dass sein Mitarbeiter seit 2 Wochen nicht mehr als Arzt, sondern nun als Jurist tätig ist, kann dieser die GR für seinen Mitarbeiter X abbestellen. Somit werden dem Mitarbeiter alle Berechtigungen, welche er als Arzt benötigte, entzogen.

RBAC vs. ABAC

RBAC Definition

Role Based Access Control (RBAC) ist eine Methodik zur korrekten Berechtigungsverwaltung in einer IT-Infrastruktur, z.B. im dortigen IAM. Mit RBAC werden Berechtigungen nicht auf einzelne Identitäten gesetzt, sondern anhand von definierten Rollen vergeben. Diese Rollen können sich dann auf Standort, Abteilung, Funktionen oder Kostenstelle der Identität beziehen.

RBAC ist sehr flexibel, so ist es je nach Bedarf möglich nur eine, aber auch mehrere Rollen einer Identität zuzuteilen. Ein solches Rollenmodell bietet einem Unternehmen zudem auch Transparenz, da die Namensvergabe verständlich gehalten werden kann (hinsichtlich Governance auch von Vorteil), aber auch Sicherheit, da man so eine kontrollierte Berechtigungsverwaltung hat.

Aufgrund der arbeitsintensiven Erstellung solcher Rollen, wäre es aber gerade für kleinere Unternehmen weniger aufwendig, die Berechtigungen manuell zu verwalten.

Wenn eine Identität solchen eine übergreifende Rolle zugewiesen bekommt, kann ein IAM-System in Hintergrund dafür sorgen, dass die Identität in allen Anwendungen die mit der Rolle verbundenen Berechtigungen erhält.

ABAC Definition

Attribute Based Access Control (ABAC) ist eine Methodik zur korrekten Berechtigungsverwaltung in einer IT-Infrastruktur, z.B. im dortigen IAM. Mit ABAC werden Berechtigungen nicht auf einzelne Identitäten gesetzt, sondern anhand von eines oder mehreren ihrer Attribute vergeben. Diese Attribute können dann z.B. Standort, Abteilung, Funktionen oder Kostenstelle der Identität sein.

Mit der Hilfe eines IAM-Systems kann ABAC bspw. mit einem Attribute Mapper verwendet werden. Solch ein Attribute Mapper verknüpft dann die Felder und Variablen aus einem Quellsystem mit den entsprechenden Attributen des IAM-Systems. Man kann dann somit z.B. festlegen, dass einer Identität mit dem Attribut Abteilung = Buchhaltung die nötigen Berechtigungen für eine ERP-Software zugewiesen werden.

Unterschied

Während RBAC Berechtigungen basierend auf Benutzerrollen verwaltet, nutzt ABAC Attribute wie Standort, Abteilung oder Funktion einer Identität für die Verwaltung.

RBAC bietet eine Simplizität, da Rollen einfach verteilt oder bestellt werden können und normalerweise einen verständlichen Namen besitzen. Es kann bei RBAC aber dazu führen, dass es zu einer «Role Explosion» kommt, das heisst es werden hunderte, tausende Rollen erstellt, da bei jeder Berechtigungsabweichung eine neue Rolle erstellt wird.

Mit ABAC kann man sehr genau und spezifisch Berechtigungsabweichungen verwalten. Es ist jedoch aufwendig, die verschiedenen Rules zu definieren, vor allem wenn man von null beginnen muss.

Role mining

Beim Role mining wird analysiert welche Berechtigungen die verschiedenen Identities haben. Das heisst es wird ermittelt, welche Berechtigungen in eine Rolle zusammengefasst werden können.

Fürs Role mining gibt es verschiedene Tools, manche besser, manche schlechter. Dabei gibt es Tools, welche lediglich tabellarisch die Analyse aufzeigen sowie aber auch andere welche in Form von farbigen Grafiken dargestellt werden.

Darunter gibt es auch Tools, welche sogenannte "What-If-Szenarien" aufzeigen können. Sprich, sie können im Vorhinein aufzeigen welche Auswirkungen bestimmt Rollenänderungen haben können.

Top-Down vs. Bottom-Up

Bei der RBAC-Methode **Top-Down** wird davon ausgegangen, dass die Identities im Unternehmen grundsätzlich zu viele Berechtigungen besitzen. Sprich, mehr als sie für ihre Arbeit benötigen. Somit wird als nächstes analysiert, welche Berechtigungen die jeweiligen Identities in ihrer Funktion benötigen. Dies tut man, indem man dokumentiert, was die Identity tagtäglich für Berechtigungen benötigt, sich mit den Managern von den Identities austauscht, System Owner fragt was für die Applikationen für Berechtigungen notwendig sind oder Inkonsistenzen und unerlaubten Zugriff identifiziert. Somit können dann Rollen bezogen auf die Funktionen der Identities erstellt werden.

Bottom-Up wird typischerweise mittels Role mining-Technik gemacht. Aus einzelnen Berechtigungen wird analysiert welche Rollen für bestimmte Mitarbeitergruppen oder Abteilungen gebildet werden können.

Lifecycle

Ein Lifecycle beschreibt im IAM-Umfeld die «Lebensdauer» einer Person/Identity/eines Objekts in einem Unternehmen. Sprich, vom Eintrittsdatum bis zum Austrittsdatum, dazwischen passierende Beförderungen oder Degradierungen, aber auch interne Stellenwechsel, gehören ebenfalls dazu. Grundsätzlich haben alle Objekte in einem IAM-System einen Lifecycle, von der Entstehung über die Veränderung bis zur Löschung/Archivierung.

Beispiel: **Identity Lifecycle**

Joiner: Ein Mitarbeiter tritt einem Unternehmen bei und wird daher im HCM-System aufgenommen. Von da aus gelangt er dann ins IAM-System.

Mover: Der Mitarbeiter wechselt im Verlaufe seiner Amtszeit möglicherweise die Abteilung und nimmt eine andere Funktion wahr. Die Änderung wird im HCM-System vorgenommen und ebenfalls ins IAM-System synchronisiert.

Leaver: Schlussendlich verlässt der Mitarbeiter das Unternehmen. Der Austritt wird ins HCM-System aufgenommen und wieder mit dem IAM-System synchronisiert.

Durch die Implementation eines Identity Lifecycles im IAM-System werden beim Joiner automatisch die benötigten Berechtigungen und Konten erteilt. Die Änderungen beim Mover werden ebenfalls automatisiert ausgeführt und beim Leaver werden wieder automatisch alle Berechtigungen und Konten entzogen, bevor die Identität deaktiviert/gelöscht wird. Durch den Identity Lifecycle verhindert man also «Account-Leichen» und erhält einen Automatismus.

IAM Prozesse, Vorgängen und Workflows

Es gibt 4 Kategorien, in welche die Vorgänge eines IAM-Systems unterteilt werden können:

1. Identitätsverwaltung
2. Berechtigungsverwaltung
3. Anlieferung & Provisionierung
4. Governance / Compliance

Ein Prinzip, welches sich durch mehrere Kategorien zieht, sind die 3 Prozesse: Joiner, Mover & Leaver.

In der **Identitätsverwaltung** geht es zum einen um Mitarbeiter-Identitäten, aber auch um technische Identitäten und OUs. Bspw. werden Mitarbeiter-Identitäten zuerst vom SAP importiert und danach im IAM angelegt (Joiner). Es kann dann passieren, dass ein Mitarbeiter eine Stelle/Namen/Abteilung oder Ähnliches wechselt oder temporär das Unternehmen verlässt und somit eine "Mutation" stattfinden muss (Mover). Wenn ein Mitarbeiter dann endgültig das Unternehmen verlässt, muss dieser entweder gelöscht oder archiviert werden, wodurch die Accounts dieser Identität entfernt werden und sie keinerlei Berechtigung mehr hat (Leaver).

Bei der **Berechtigungsverwaltung** werden Rollen, Rollenbeziehungen oder Zielsystemberechtigungen verwaltet. Bspw. wird eine GR im IAM angelegt (Joiner). Dieser können dann während ihrer Existenz Zielsystemrollen hinzugefügt und wieder entzogen werden (Mover). Wenn sie nicht mehr benötigt werden, können sie gelöscht werden (Leaver). Die Berechtigungsverwaltung ist zusammenhängend mit der Identitätsverwaltung. Denn durch den Mover-Prozess in der Identitätsverwaltung werden meistens auch Änderungen in der Berechtigungszuteilung passieren.

Bei der Kategorie **Anlieferung & Provisionierung** spricht man eigentlich von den 2 Themen: Anlieferung aus Quellsystemen und Provisionierung in Zielsysteme. Bei der Provisionierung in die Zielsysteme werden dabei ZRs an die über die Identitäten automatisch erstellten Accounts zugeteilt. Diese beinhalten dann die Zielsystemberechtigungen, welche den Accounts die benötigten Rechte liefern.

Eine weitere Kategorie ist **Governance / Compliance**. Hier geht es um Genehmigungen, Regeln, Risikobewertung, Attestierung, Re-Zertifizierung, Berichtswesen und Archivierung. Bei den Genehmigungen sind die Workflows bspw. für die Bestellung einer Rolle gemeint, in welchen das 4-Augen-Prinzip zum Zug kommt. Da die ganze Abhandlung nachvollziehbar sein soll, müssen bei einer Bestellung zudem noch Begründungen angeben werden. Weitere angewendete Prinzipien sind Segregation of Duties (SoD), was so viel ist wie die unvereinbaren Funktionen zu prüfen, und das Least-Privilege-Prinzip, sprich, man darf nur so viele Berechtigungen wie nötig haben.

<u>Beispiel 1:</u>
Bei einer Attestierung kann herausgelesen werden, dass die GR X keinen RM hat. Dies kam zustande, da der bisherige RM das Unternehmen verlassen hat und der Leaving-Prozess nicht korrekt funktioniert hat. Denn die GR hätte so mutieren sollen, dass sie einen neuen RM erhält.

<u>Beispiel 2:</u>
Mitarbeiter X benötigt Zugriff auf ein ZS. Er bestellt also eine GR, welche durch das 4-Augen-Prinzip bestätigt wird, und erhält somit einen Account für das Zielsystem, welcher wiederum die bestellten Berechtigungen enthält.

Organisatorische Begriffe

Attestierung

Attestierungen dienen im IAM-Umfeld dazu überprüfen zu können, ob bspw. Mitarbeiter X die Berechtigung Y noch benötigt oder nicht. Sprich, ein Vorgesetzter oder/und ein Rollenmanager sollen bescheinigen, ob nach dem Need-To-Know-Prinzip die Berechtigung/Rolle noch für die tägliche Arbeit eines Mitarbeiters notwendig ist. Falls ja, soll die Attestierung genehmigt werden und der Mitarbeiter kann seine Rolle/Berechtigung behalten. Falls nein, wird die Rolle/Berechtigung dem Mitarbeiter entzogen.

Nebst dem Need-To-Know-Prinzip sind Attestierungen auch aufgrund der «Generellen Rahmenbedingungen» zwingend nötig. Treiber dahinter ist die DSGVO oder Firmen-interne Personen/-gruppen wie z.B. die IT Security.

Re-Zertifizierung

Im IAM-Umfeld beschreibt die Re-Zertifizierung den Prozess, Attestierungen in festgelegten Zeitabständen durchzuführen. Die Re-Zertifizierung sorgt also über automatisierte Prozesse und Genehmigungsworkflows für eine Minderung der Sicherheitsrisiken, die von inaktiven Accounts ausgehen.

Beispielsweise muss also die verantwortliche Person einer externen Identität alle 3 Monate bestätigen, ob dieser externe Mitarbeiter noch für das Unternehmen tätig ist und somit die Rolle XY noch benötigt.

SoD

Segregation of Duties (SoD) bedeutet, dass die Berechtigungen/Rollen (Bestellungen) sich nicht im Widerspruch befinden dürfen. Sprich, Person X darf nicht in einer Gruppe A und B sein, wenn sich diese widersprechen. Diese Regeln werden von Fachabteilungen definiert.

Reporting

Reporting dient dazu, eine Übersicht von bspw. Berechtigungen einer Identität zu bieten.

Weitere Themen

PAM

Privilegierter Zugriff beschreibt den Besitz von Zugriffsberechtigungen, welche über den eines Standardbenutzers hinausgehen. Somit können Infrastrukturen gesichert werden. Dieser Zugriff kann Personen/Accounts (Domain-/Local Admin, Superuser) oder auch nicht menschlichen Accounts (Service-Account, Secret) zugeteilt werden.

Solche Accounts bieten aber natürlich (vor allem, wenn ihre Passwörter über einen längeren Zeitraum unverändert bleiben) ein grosses Sicherheitsrisiko. Mit PAM kann nun dafür gesorgt werden das Sicherheitsrisiko zu minimieren. PAM gilt als eine IT-Security-Struktur zur Kontrolle, Überwachung, Sicherung und Prüfung all dieser privilegierten Accounts. Ausserdem beruht es auf dem Need-To-Know-Prinzip, sprich, jede Identität soll nur so viele Berechtigungen erhalten, wie sie auch benötigt.

Im Hinblick auf Compliance ist PAM ein wichtiger Punkt. Zwar sind die Erkennung und Überwachung von verdächtigten Ereignissen in einem System wichtig, jedoch bleibt ein Unternehmen ohne Klarheit über das grösste Risiko trotzdem noch gefährdet. Mit PAM können nun all diese Aktivitäten aufgezeichnet und protokolliert werden. Zusätzlich gibt es oft die Möglichkeit mit PAM «rotierende» Passwörter zu setzen. So weiss nicht einmal der Admin selbst, wie sein Passwort lautet.

PAM wird hier und dort teils auch als PIM (Privileged Identity Management) oder PAS (Privileged Access Security) bezeichnet.

Authentication

Authentifizierung (engl. Authentication / kurz AuthN) beschreibt den Vorgang der Überprüfung einer Identität eines Benutzers, welcher sich an ein System anmelden möchte.

Aus der Perspektive des Systems geht es darum herauszufinden, wer sich am System anmelden möchte.

Bei der Überprüfung wird zuerst ein Nachweis, eine Authentisierung, statt, sprich, der Benutzer muss bspw. seinen Benutzernamen eingeben. Als Nächstes muss dieser noch bspw. ein Passwort eingeben, um zu beweisen, dass er auch wirklich die Identität ist, die er angibt zu sein.

Methoden

- personifiziertes Objekt:
    - Smartphone
    - SMS
    - Authenticator App

    - physischer Schlüssel
    - Client Zertifikat
- etwas Geheimes kennen:
    - Passwort / One-Time-Password (OTP)
    - PIN
    - Sicherheitsfrage
    - Captcha
- bestimmter Ort
    - LAN
    - Geotracking

MFA / 2FA

Multi Factor Authentication oder Two Factor Authentication beschreibt das Prinzip, dass sich eine Person, welche sich an einem System authentifizieren lassen möchten, mind. noch eine zusätzliche Authentifizierungsmethode verwenden muss, welche aus einer anderen «Kategorie» stammt. Sprich, man kann nicht ein Passwort festlegen, und dann als weiteren Faktor eine PIN verwenden, sondern müsste dann bspw. eine Authenticator App verwenden.

Ziel dabei ist es eine höhere Sicherheit bieten zu können, da bspw. beim Verlust des Passworts sich ein Dritter ohne den Besitz des zusätzlichen Faktors nicht anmelden kann.

Authorization

Autorisierung (engl. Authorization / kurz AuthZ) folgt nach der Authentifizierung. Hierbei wird überprüft, welche Berechtigungen ein Benutzer hat, bspw. auf welche Programme oder Dokumente er zugreifen darf.

Aus der Perspektive des Systems geht es darum herauszufinden, was die angemeldete Identität im System tun oder sehen darf.

Single Sign-on / Single Sign-out

Mit Single Sign-on (SSO) kann ein Benutzer nach einer einmaligen Authentifizierung an einem System auf alle Dienste in diesem, für welche er zugriffsberechtigt ist, zugreifen, ohne sich dabei jedes Mal zusätzlich anmelden zu müssen.

Das Pendant dazu ist Single Sign-out (oder Single Sign-off), bei welchem sich ein Benutzer mit einer einzigen Abmeldung im System auf allen Diensten gleichzeitig abmelden kann, ohne dabei sich überall einzeln abmelden zu müssen.

Identity Federation

Identity Provider

Ein Identity Provider, kurz IdP, ist ein Dienst, welcher Identitäten (Personen) speichert und verifiziert. Es ist also so zusagen ein zentrales Zugangssystem.

Ein IdP kann in der Cloud, aber auch intern gehostet werden. Meist kommt ein IdP in Verknüpfung mit SSO (Single Sign-on) daher.

Diese Identitäten sind dann somit über mehrere Plattformen/Systeme verfügbar. Deshalb nennt man sie auch «federated identities». Der IdP muss federated identities sicher in einer Datenbank speichern und diese als Identity Provider den Service Providern zur Verfügung stellen, wenn dies von der jeweiligen Identität (Person) «gefordert» wird.

Wenn sich eine Person nicht überall neu registrieren möchte, um dann anschliessend unzählige Accounts pflegen zu müssen, kann sie sich mittels eines Identity Providers bei den jeweiligen Service Providern anmelden.

Beispiele für **Identity Provider** sind:

- Google
- Microsoft
- Facebook
- Apple
- Fitbit

Beispiele für **Service Provider** von Google Sign-In sind:

- SAMSUNG Account (TV)
- Adobe
- Digitec Galaxus Oauth CH

Wie funktioniert das Ganze?

Der IdP kommuniziert mittels Web-Services mit standardisierten Verfahren wie SAML oder Datenformaten wie OAuth.

Dabei gibt es drei hauptsächliche Schritte bei einem Verbindungsaufbauversuch:

1. **Authentication** → Hierbei wird offenbart, welches Gerät / welcher Benutzer die Anfrage stellt
2. **Attribution** → Es werden alle relevanten, von der Person zugestimmten Daten übergeben
3. **Authorization** → Hier wird entschieden ob die Anfrage gewährt wird oder nicht

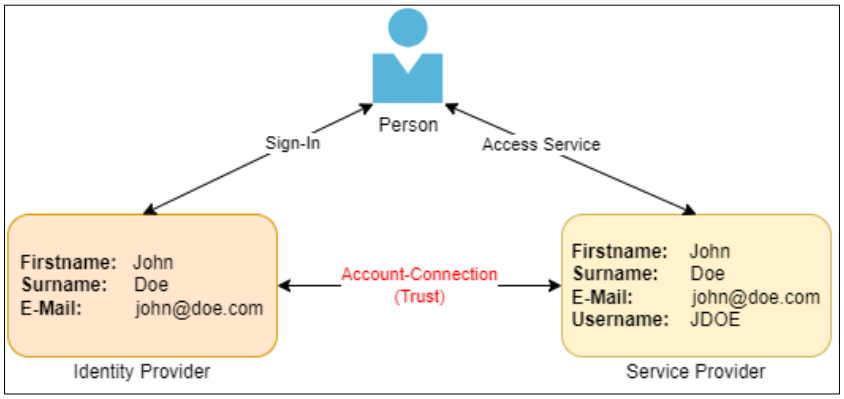

Abbildung 4: Beispiel: Identity Federation (Dätwyler, 2022)

Passwortverschlüsselung mit Hash & Salt

Ein wichtiges Kriterium für eine Hash-Funktion ist, dass sie aus einem Eingabewert zwar einen Ausgabewert errechnet, dieser jedoch komplett anders ist. Jedoch muss bei jedem Aufruf desselben Eingabewertes wiederum auch derselbe Ausgabewert errechnet werden. Die Verschlüsselung mittels Hash ist zudem lediglich 1-wegig. Sprich, man kann unter keinen Umständen den ursprünglichen Eingangswert errechnen. Somit kann nicht einmal der Systemadministrator, geschweige denn ein Sicherheitsexperte das Passwort entschlüsseln.

Wird ein Passwort erzeugt oder gespeichert, wird zuerst aus der Hash-Funktion ein Hash-Wert berechnet. Im System wird nur der berechnete Hash-Wert gespeichert. Das ursprüngliche Passwort wird somit nicht im System gespeichert. Wenn sich nun an einem System angemeldet wird, wird aus dem eingegebenen Passwort nun wieder anhand der gleichen Hash-Funktion derselbe Hash-Wert berechnet. Somit wird dann der Hash-Wert von der Eingabe des Hash-Werts des vorher gespeicherten Passwortes verglichen.

Hier ein, sicherheitstechnisch gesehen, schlechtes Beispiel anhand der Quersumme der PIN:

User	PIN	Hash-Wert | PIN	Problem?
Alice	123456	21	kein Problem
Bob	456789	**39**	Kollision!
Charlie	987654	**39**	Kollision!

Das Problem der Kollision entsteht in diesem Beispiel dann, wenn verschiedene Passwörter den gleichen Hash-Wert haben – was durchaus möglich ist. Dabei könnten also mehrere Eingaben als korrekt angesehen werden.

Um solch eine Kollision zu verhindern, werden heute oft «Secure Hash Algorithm (SHA)»-Verfahren verwendet, welches unter anderem das MD5-Verfahren abgelöst hat.

Wenn Alice und Bob also beide dasselbe Passwort haben (bspw. 123456), dann ist auch bei beiden Passwörtern der Hash-Wert identisch. Wenn sich nun jemand Zugriff auf eine grosse Anzahl von Benutzer-IDs und den jeweiligen, dazugehörigen, mit Hash verschlüsselten Passwörter verschafft, kann dieser möglicherweise den Schluss daraus ziehen, dass Passwörter mit demselben Hash-Wert gleich sind. Wenn er nun mit einem dieser Benutzer-IDs eine Brute-Force-Attacke ausführt und das Passwort erfährt, weiss er, dass er direkt das Passwort von mehreren Accounts geknackt hat.

Wenn man nun das erstellte Passwort aber mit Salt erweitert, wird bei jedem Passwort ein neuer Zufallswert (Salt) hinzugefügt, welcher gemeinsam mit dem Benutzer zusammen gespeichert wird. Der Hash-Wert wird nun also nicht mehr allein auf Basis des Passworts berechnet, sondern des Passworts inkl. Salt. Bei der Authentifizierung wird dann automatisch nach Eingabe des Passworts der gleiche Salt-Wert am Passwort angehängt, woraus dann wieder der Hash-Wert generiert wird.

User	PIN	Hash-Wert | PIN	Salz	PIN + Salt	Hast-Wert | PIN + Salt
Alice	123456	**21**	132	123456132	**27**
Bob	123456	**21**	456	123456456	**36**

Abkürzungsverzeichnis

2FA ..... Two Factor Authentication
ABAC ..... Attribute Based Access Control
AuthN ..... Authentication
AuthZ ..... Authorization
CIAM ..... Consumer Identity & Access Management
CISO ..... Chief Information Security Officer
GR ..... Geschäftsrolle (Business role)
HCM ..... Human Capital Management
IAG ..... Identity & Access Governance
IAM ..... Identity & Access Management
IdP ..... Identity Provider
ILM ..... Identity Lifecycle Management
MD5 ..... Message-Digest Algorithm 5
MFA ..... Multi Factor Authentication
OTP ..... One-Time-Password
PAM ..... Privileged Access Management
PAS ..... Privileged Access Security
PIM ..... Privileged Identity Management
RBAC ..... Role Based Access Control
RM ..... Rollenmanager
SCIM ..... System for Cross-domain Identity Management
SHA ..... Secure Hast Algorithm
SoD ..... Segregation of Duties
SSO ..... Single Sign-on
ZR ..... Zielsystemrollen
ZS ..... Zielsystem

Glossar

Da die meisten Begriffe direkt beschrieben wurden, ist dieses Glossar mehr ergänzend anzusehen.

Begriffe	Definition
Access Certifications	Dieser Begrifft steht für den Vorgang, in welchem ein Manager oder System Owner dafür schaut, dass die Personen (Identities) lediglich Zugriff auf das haben, was sie auch wirklich benötigen. Zudem wird hierbei mittels Governance nochmals überprüft, ob die Personen immer noch ihre Berechtigungen benötigen. Dafür wird bspw. ein Mail an alle Owner versendet, in welchem gefragt wird, ob eine bestimmte Person noch eine gewisse Berechtigung benötigt.
Access Request	Ein Access Request ist ein User-Interface, welches einer Person ermöglicht Zugriffsrechte selbst zu bestellen.
Auditing	Beim Auditing muss bspw. eine Auswertung zusammengestellt werden, indem alle Accounts inkl. Zugriffsberechtigungen aufzufinden sind. Somit kann überprüft werden, ob zu viele Identities vorhanden sind, oder fasche Zugriffsberechtigungen zugeteilt wurden.
Business role	Eine GR ist eine Bündelung von Rollen/Berechtigungen. Eine solche GR kann z.B. den Namen «Arzt» tragen.
Chief Information Security Officer (CISO)	Ein CISO bezeichnet die Rolle des Gesamtverantwortlichen für Informationssicherheit in einer Organisation.
Connection string	In der Datenverarbeitung ist ein Connection string eine Zeichenfolge, die Informationen über eine Datenquelle und die Mittel zum Herstellen einer Verbindung zu ihr angibt.
Consumer Identity & Access Management (CIAM)	CIAM wird für die Identifikation, Authentifizierung und Autorisierung von Kunden, Geräten und externen Organisationen verwendet. CIAM bietet für die Consumer nicht nur eine höhere Benutzerfreundlichkeit, sondern auch ein einfacheres und sichereres Registrieren für einen gewissen Service. Für die IAM-Admins wird das Lifecycle Management von verschiedensten Identities vereinfacht.

Entitlement Management	Hierbei geht es zum einen darum, die Zugriffsrechte oder Aufgaben von bestimmten Identities einzusehen. Dabei kann man sich unter anderem die Account-Typen, Rollen und Gruppenmitgliedschaften der Identities anzeigen lassen. Weiter geht es aber auch zusätzlich noch um die Setzung bzw. Änderung von Berechtigungen.
Fulfillment	Es geht um die Provisionierung vom Erstellen, Ändern (Provisioning) und Löschen (Deprovisioning) von Objekten (Accounts, Geschäftsrollen etc.), welche durch das IGA-Tool initiiert wurden, und die Weitergabe an die Zielsysteme.
Human Capital Management (HCM)	Ein Personalinformationssystem ist ein personenbezogenes Informationssystem, das der Erfassung, Speicherung, Verarbeitung, Pflege, Analyse, Besetzung, Verarbeitung, Übertragung und Anzeige von Informationen dient, die die Personalverwaltung betreffen.
Identity Lifecycle Management (ILM)	ILM beschreibt die «Lebensdauer» einer Person/einer Identity in einem Unternehmen. Sprich, vom Eintrittsdatum bis zum Austrittsdatum. Dazwischen passierende Beförderungen oder Degradierungen, aber auch interne Stellenwechsel, gehören ebenfalls dazu.
Identity Management	Während **Entity** etwas Existierendes oder einen Konkreten Gegenstand darstellt, ist die **Identity** eine alleinige Darstellung einer Entity (einzelne Person). Ein **Account** verbindet dann die Identity mit einem Unternehmensnetzwerk.
IGA-Tool	Identity Governance and Administration ist ein infosec Mechanismus (information security), welcher Identities mit speziellen Zugangsberechtigungen zusätzlich schützt.
Least-Privilege-Prinzip	Während das Need-to-Know-Prinzip sich darauf bezieht, Informationen nur mit einem möglichst kleinen Kreis von Personen zu teilen, deckt das Least-Privilege-Prinzip darüber hinaus auch nicht-menschliche User und Geräte ab.
Rollenmodell	Ein Rollenmodell beschreibt ein Konzept eines Unternehmens, welches die Methodik RBAC in einem IAM-System umsetzen möchte.
System for Cross-domain Identity Management (SCIM)	SCIM ist ein Standard zur Automatisierung des Austauschs von Benutzeridentitäts-Informationen zwischen Identitätsdomänen oder IT-Systemen.
Workflows	Mit Hilfe von Workflows können bspw. die Abläufe in einem Unternehmen wie folgt geregelt werden: Wenn ein Mitarbeiter neue Zugriffsrechte mittels *Access Request* bestellen möchte, wird die Zuteilung erst dann erfolgen, wenn ein Vorgesetzter diese Anfrage bewilligt.

Literaturverzeichnis

Dätwyler, M. (2022). *Abbildung 4: Beispiel: Identity Federation (Eigene Herstellung).*

Dätwyler, M. (2023). *Abbildung 2: Analogie: Governance Korrelation (Eigene Herstellung).*

Dätwyler, M. (2023). *Abbildung 3: IAM als Drehscheibe (Eigene Herstellung).*

Rise, D. (2020). Identity and Access Management. Shutterstock. Von https://images.computerwoche.de/bdb/3217695/1200x.jpg abgerufen

Abbildungsverzeichnis

