Identity & Access Management

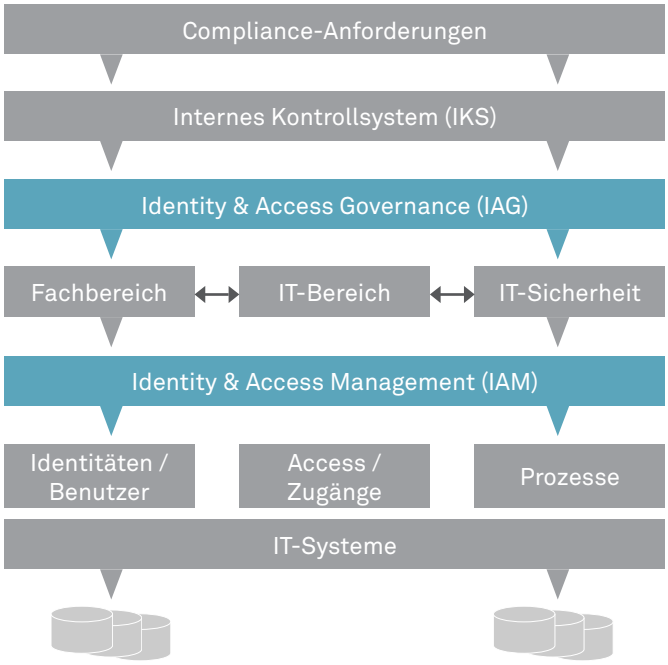
Zugriffe verwalten, steuern und überwachen

Die Verwaltung digitaler Identitäten erfolgt häufig dezentral und spezifisch je Anwendung. Das Identity & Access Management ist als technisches Rückgrat der Sicherheitsinfrastruktur jedes Unternehmens mehr als ein Werkzeug, wenn es auch Prozesse und Personen berücksichtigt.

Definition

Identity & Access Management (IAM) dient dem Schutz wichtiger Informationen vor unberechtigtem Zugriff. Die Anforderungen können hierzu extern durch Gesetze oder intern durch Policies vorgegeben sein. Durch Authentifizierung werden im Access Management Personen identifiziert. Mittels Autorisierung wird definiert, welche Dienste diese dann nutzen können.

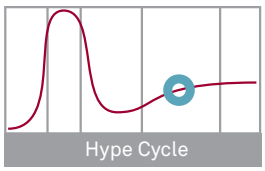
Durch Provisionierung werden diese Informationen zielgerecht zur Verfügung gestellt, und durch Kontrollen wird das Zugriffsverhalten überwacht. Wenn hierbei die Nachweispflicht im Fokus steht, etwa aufgrund regulatorischer Anforderungen, wird auch von Identity & Access Governance gesprochen. Wurden bisher häufig Berechtigungen für Benutzer für jede Anwendung separat vergeben, wird diese



Aufgabe heute immer öfter zentral gesteuert und überprüft. Dazu wird das IAM als strategischer Service-Baustein in die gesamte Unternehmensorganisation eingebettet. Neue gesetzliche Anforderungen bezüglich Nachweispflichten, aber auch neue Service-Szenarien, zum Beispiel durch die wachsende Nutzung und den steigenden Integrationsbedarf von Cloud-Diensten oder mobilen Anwendungen, bringen neue Herausforderungen mit sich.

Reifegrad

IAM liegt wohl-definiert und einsatzbereit vor. Die Unterstützung durch Technologien ist vollständig



vorhanden. Eine Optimierung kann durch geeignete Wahl der Werkzeuge, durch abgestimmte Prozesse und deren gesamthafte Integration im Unternehmen erreicht werden.

Marktübersicht

Auf dem Markt der IAM-Toolhersteller hat es in den letzten Jahren wichtige Weiterentwicklungen gegeben, um diesen neuen Herausforderungen gerecht zu werden: So wurden zur Unterstützung der Nachweispflichten Governance-Module entwickelt, wie beispielsweise SAP GRC oder von Beta Systems; aber auch neue Hersteller, wie SailPoint oder Aveksa, punkten mit entsprechenden eigenen Lösungen. Daneben haben viele Hersteller zur Weiterentwicklung von Standards, wie etwa der Security Assertion Markup Language (SAML) oder dem offenen Autorisierungsprotokoll OAuth, beigetragen, um Cloud-Services integrieren zu können, und diese in ihren Produkten umgesetzt, zum Beispiel CA oder NetIQ.

IAM kann somit als eigener Service betrieben werden, damit Personen anderer Organisationen, wie etwa Partnern, Lieferanten oder Kunden, bei Bedarf einfacher Zugriff auf interne Dienste gewährt werden kann – bei vollständiger Beibehaltung der eigenen Kontrolle.

Referenzszenario

Auf technischer Ebene wird ein Identity-Management-System meist aus mehreren Datenquellen versorgt, die die relevanten Personendaten beinhalten.

Solche Datenquellen können ein Personalverwaltungssystem oder auch Systeme von Partnern sein. Diese Daten werden dann transformiert und an die Erfordernisse angepasst. In Analogie zum Data Warehouse wird hierbei auch von einem Identity Warehouse gesprochen. Diese Daten können durch geeignete Integration oder Föderation den Zielanwendungen zur Verfügung gestellt werden. Zur Administration gibt es somit nur noch eine definierte Stelle und die Anwender verwenden nur noch einen einzigen Login-Namen und ein Passwort. Zur Unterstützung der Geschäftsprozesse erfolgt eine gesamtheitliche Ende-zu-Ende-Betrachtung, sowohl des Benutzerlebenszyklus als auch der Geschäftsanwendungen. Somit können Personen beginnend ab deren Einstellung bis hin zum Verlassen des Unternehmens effizient verwaltet werden. Eine geeignete Modellierung stellt sicher, dass diesen Personen entsprechend ihrer organisatorischen Rollen die zugehörigen Berechtigungen eingeräumt und wieder entzogen werden können.

Business Impact

Beim Identity & Access Management ist nicht nur das eingesetzte Werkzeug wesentlich, sondern es betrifft Personen, Prozesse und die Anwendungen, die die Personen verwenden, um ihre Prozesse umzusetzen. Daher hat Identity & Access Management Auswirkungen auf die gesamte Organisation. Die Komplexität darf daher nicht unterschätzt werden.

Pro	Contra
Zentrale Steuerung und Nachweisbarkeit der Berechtigungsvergabe	Die Ablösung von dezentralen Berechtigungslösungen ist zunächst mit Aufwänden verbunden
Konsistente Stammdaten führen zu Administrationsvereinfachung	
Entlastung des Helpdesks	Hoher Abstimmungsbedarf

msg systems ag
Robert-Bürkle-Straße 1 | 85737 Ismaning/München
Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113
www.msg-systems.com | info@msg-systems.com

Stand: September 2013
http://www.msg-systems.com/techrefresh
XT-290-1309-1